RackSwitch™ G8000
Command Reference

Version 6.0

Part Number: BMD00128, September 2009

BLADE
NETWORK TECHNOLOGIES

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
www.bladenetwork.net

Contents

Preface 9
Who Should Use This Book 10
How This Book Is Organized 11
Typographic Conventions 12
How to Get Help 14

ISCLI Basics 15
ISCLI Command Modes 15
Global Commands 18
Command Line Interface Shortcuts 20
Command Abbreviation 20
Tab Completion 20
User Access Levels 21
Idle Timeout 22

Information Commands 23
System Information 25
SNMPv3 System Information 25
SNMPv3 User-based Security Model User Table Information 27
SNMPv3 View Table Information 28
SNMPv3 Access Table Information 29
SNMPv3 Group Table Information 31
SNMPv3 Community Table Information 31
SNMPv3 Target Address Table Information 32
SNMPv3 Target Parameters Table Information 33
SNMPv3 Target Parameters Table Index Information 33
SNMPv3 Notify Table Information 34
SNMPv3 Dump Information 35
General System Information 36
Show Syslog Messages 37

User Status 37
Stacking Information 39
Show Stacking Switch Information 41
Layer 2 Information 43
Forwarding Database Information 44
Show All FDB Information 45
Clearing Entries From the Forwarding Database 46
Link Aggregation Control Protocol Information 47
Link Aggregation Control Protocol 47
Layer 2 Failover Information 49
Layer 2 Failover information 49
802.1X Information 50
Trunk Group Information 52
Trunk Group 52
VLAN Information 53
Layer 3 Information 54
ARP Information 55
Show All ARP Entry Information 56
IGMP Multicast Group Information 57
IGMP Group Information 58
IGMP Multicast Router Information 59
IP Information 59
QoS Information 61
QoS DSCP Information 62
Access Control List Information 64
Access Control List Information 64
Port Information 65
Interface Link Information 66
Interface Transceivers 67
Information Dump 67

Statistics Commands 69

Port Statistics 70
Port 802.1X Authenticator Statistics 71
Port 802.1X Authenticator Diagnostics 73
Port Bridging Statistics 75
Port Ethernet Statistics 76
Port Interface Statistics 78
Port IP Statistics 81
LACP Statistics 82
Link Statistics 83

Layer 2 Statistics 84
Forwarding Database Statistics 85
Layer 3 Statistics 86
ARP Statistics 87
IGMP Statistics 88
Access Control List Statistics 90
ACL Statistics 90
Management Processor Statistics 91
TCP Statistics 91
UDP Statistics 92
CPU Statistics 93
SNMP Statistics 94
Statistics Dump 98
Statistics Dump Output Example 98

Configuration Commands 99
Viewing and Saving Changes 101
Saving the Configuration 101
System Configuration 102
System Host Log Configuration 104
SSH Server Configuration 105
RADIUS Server Configuration 106
TACACS+ Server Configuration 107
NTP Server Configuration 110
System SNMP Configuration 110
SNMPv3 Configuration 113
User Security Model Configuration 115
SNMPv3 View Configuration 116
View-Based Access Control Model Configuration 117
SNMPv3 Group Configuration 118
SNMPv3 Community Table Configuration 119
SNMPv3 Target Address Table Configuration 120
SNMPv3 Target Parameters Table Configuration 121
SNMPv3 Notify Table Configuration 122
System Access Configuration 123
HTTPS Access Configuration 124
Management Network Configuration 125
User Access Control Configuration 126
System User ID Configuration 127
Port Configuration 128
Port Link Configuration 129

Temporarily Disabling a Port 130

Port ACL Configuration 131

Stacking Configuration 132

Stacking Switch Configuration 133

Master Switch Interface Configuration 134

Backup Switch Interface Configuration 135

Port Mirroring 136

Layer 2 Configuration 137

802.1X Configuration 138

802.1X Global Configuration 138

802.1X Guest VLAN Configuration 140

802.1X Port Configuration 141

FDB Configuration 143

Trunk Configuration 143

IP Trunk Hash Configuration 145

Link Aggregation Control Protocol Configuration 146

LACP Port Configuration 148

Layer 2 Failover Configuration 149

Failover Trigger Configuration 149

Failover Manual Monitor - Monitor Configuration 150

Failover Manual Monitor - Control Configuration 151

VLAN Configuration 152

Layer 3 Configuration 154

ARP Configuration 155

IGMP Snooping Configuration 156

IGMP Static Multicast Router Configuration 158

Domain Name System Configuration 159

Quality of Service Configuration 160

802.1p Configuration 160

DSCP Configuration 161

Access Control Configuration 161

Access Control List Configuration 162

Ethernet Filtering Configuration 162

IP version 4 Filtering Configuration 164

TCP/UDP Filtering Configuration 165

Packet Format Filtering Configuration 166

ACL Group Configuration 167

ACL Metering Configuration 167

ACL Re-Mark Configuration 168
Re-Marking In-Profile Configuration 168
Update User Priority Configuration 168
Re-Marking Out-of-Profile Configuration 169
Configuration Dump 170
Saving the Active or Backup Switch Configuration 170
Restoring the Active or Backup Switch Configuration 170
Show Active and Backup Configuration 171
Active Configuration command output 172

Operations Commands 173
Operations-Level Port Options 174

Boot Options 175
Stacking Boot commands 176
Updating the Switch Software Image 177
Loading new Software to Your Switch 178
Selecting a Software Image to run 179
Uploading a Software Image From Your Switch 179
Selecting a Configuration Block 180
Resetting the Switch 180
Accessing the BLADE OS CLI 181
Using the Boot Management menu 182
Using SNMP with Switch Images and Configuration Files 183
Loading a new switch image 184
Loading a switch configuration to the active configuration 184
Saving the switch configuration from the active configuration 185

Maintenance Commands 187
Forwarding Database Maintenance 189
ARP Cache Maintenance 190
IGMP Group Information 191
IGMP Multicast Routers Maintenance 192

Index 193

Preface

The RackSwitch G8000 *ISCLI Reference* describes how to configure and use the software with your switch. This guide lists each command, together with the complete syntax and a functional description, using the IS Command Line Interface (ISCLI).

For documentation about installing the switch physically, see the RackSwitch G8000 *Installation Guide*.

Who Should Use This Book

This *ISCLI Reference* is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the IEEE 802.1D Spanning Tree Protocol, and SNMP configuration parameters.

How This Book Is Organized

Chapter 1 "ISCLI Basics," describes how to connect to the switch and access the information and configuration commands. This chapter provides an overview of the command syntax, including command modes, global commands, and shortcuts.

Chapter 2 "Information Commands," shows how to view switch configuration parameters.

Chapter 3 "Statistics Commands," shows how to view switch performance statistics.

Chapter 4 "Configuration Commands," shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing and Port Trunking.

Chapter 5 "Operations Commands," shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The commands describe how to activate or deactivate optional software features.

Chapter 6 "Boot Options," describes the use of the primary and alternate switch images, how to load a new software image, and how to reset the software to factory defaults.

Chapter 7 "Maintenance Commands," shows how to generate and access a dump of critical switch state information, how to clear it, and how to clear part or all of the forwarding database.

"Index" includes pointers to the description of the key words used throughout the book.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping` *<IP address>* you enter **`ping 192.32.10.12`**
bold body text	Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.
`bold Courier text`	Indicates command names, options, and text that you must enter. Example: Use the **`show ip arp`** command.
braces { }	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`show portchannel {`***<1-52>***`|hash|information}`** you enter: **`show portchannel`** *<1-52>* or **`show portchannel hash`** or **`show portchannel information`**
brackets [ ]	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ip interface [`***<1-128>***`]`** you enter **`show ip interface`** or **`show ip interface`** *<1-128>*
italic text	Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Example: If the command syntax is **`show spanning-tree stp`** *<1-128>* *<1-128>* represents a number between 1-128.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `configure terminal`
vertical line |	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show portchannel {***<1-52>***|hash|information}** you must enter: **show portchannel** *<1-52>* or **show portchannel hash** or **show portchannel information**

How to Get Help

If you need help, service, or technical assistance, call Blade Network Technologies Technical Support:

US toll free calls: 1-800-414-5268

International calls: 1-408-834-7871

You also can visit our web site at the following address:

`http://www.bladenetwork.net`

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

CHAPTER 1

ISCLI Basics

Your switch is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

This guide describes the individual ISCLI commands available for the switch.

The ISCLI provides a direct method for collecting switch information and performing switch configuration. Using a basic terminal, the ISCLI allows you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the IS Command Line Interface (ISCLI) for the switch.

ISCLI Command Modes

The ISCLI has three major command modes, listed in order of increasing privileges, as follows:

- User EXEC mode
  This is the initial mode of access. By default, password checking is disabled for this mode, on console.
- Privileged EXEC mode
  This mode is accessed from User EXEC mode. A password is required to enter Privileged EXEC mode. The default password is **`enable`**. Enter **`disable`** to turn off privileged commands.
- Global Configuration mode
  This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the switch. Several sub-modes can be accessed from the Global Configuration mode. For more details, see Table 1-1 on page 16.

Each mode provides a specific set of commands. The command set of a higher-privilege mode is a superset of a lower-privilege mode — all lower-privilege mode commands are accessible when using a higher-privilege mode. Table 1-1 lists the ISCLI command modes.

Table 1-1 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
User EXEC `RS G8000>`	Default mode, entered automatically on console Exit: **`exit`** or **`logout`**
Privileged EXEC `RS G8000#`	Enter Privileged EXEC mode, from User EXEC mode: **`enable`** Exit to User EXEC mode: **`disable`** Quit ISCLI: **`exit`** or **`logout`**
Global Configuration `RS G8000(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: **`configure terminal`** Exit to Privileged EXEC: **`end`** or **`exit`**
Interface IP Configuration `RS G8000(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: **`interface ip`** *<1-128>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Interface Port Configuration `RS G8000(config-if)#`	Enter Port Configuration mode from Global Configuration mode: **`interface port`** *<port number, or range of ports>* **Note**: Enter a number of ports as follows: `interface port 2,7` **Note**: Enter a range of ports as follows: `interface port 2-8` Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Portchannel Configuration `RS G8000(config-PortChannel)#`	Enter Portchannel Configuration mode from Global Configuration mode: **`portchannel`** *<trunk group number>* **Note**: Static trunks are numbered from 1-52. LACP trunks are numbered from 53-104. Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
ACL Standard Configuration `RS G8000 (config-std-nacl)#`	Enter the Access Control List (ACL) IP Standard Configuration mode. **`access-list ip standard`** *<1-1000>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 1-1 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
ACL Extended Configuration `RS G8000 (config-ext-nacl)#`	Enter the Access Control List (ACL) IP Extended Configuration mode. **`access-list ip extended`** *<1001-65535>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
ACL MAC Configuration `RS G8000 (config-ext-macl)#`	Enter the Access Control List (ACL) MAC Extended Configuration mode. **`access-list mac extended`** *<1-65535>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
VLAN Configuration `RS G8000(config-vlan)#`	Enter VLAN Configuration mode, from Global Configuration mode: **`vlan`** *<1-4094>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Global Commands

Some basic commands are recognized throughout the ISCLI command modes. These commands are useful for obtaining online Help, navigating through the interface, and for saving configuration changes.

For help about a specific command, type the command, followed by `?` (question mark).

Table 1-2 Description of Global Commands

Command	Action
`?`	Help may be requested at any point in a command by entering a question mark (?). If nothing matches, the Help list will be empty and you must backup until entering a '?' shows the available options. Two styles of Help are provided: 1. Full Help is available when you are ready to enter a command argument (e.g. 'show ? ') and describes each possible argument. 2. Partial Help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)
`clear`	Clears statistical and log information. For example, enter **`clear ntp`** to clear all NTP statistics. Enter **`clear ?`** to view a list of commands.
`console-log`	Enables or disables console logging for the current session.
`copy`	Transfers files or writes configuration changes.
`default`	Resets a parameter to its default setting. For example, enter **`default access telnet port`** to reset the Telnet port to its default setting. Enter **`default ?`** to view a list of default commands.
`exit`	Go up one level in the command mode structure. Exit from the command line interface and log out.
`no`	Negates the argument. For example, if you enabled the logging console feature, and you want to disable it at a later time, enter **`no logging console`** to disable the logging console feature. Enter **`no ?`** to view a list of arguments that you can use with the **`no`** command.
`ping`	Use this command to verify station-to-station connectivity across the network. The format is as follows: **`ping`** *<host name>* | *<IP address>* [*tries (1-32)> [delay*]] Where *IP address* is the hostname or IP address of the device, *tries* (optional) is the number of attempts (1-32), *delay* (optional) is the number of seconds between attempts. The DNS parameters must be configured if specifying hostnames.

Table 1-2 Description of Global Commands

Command	Action
`[no] prompting`	Enables or disables CLI prompts. Prompts allow you to step through complex configurations, and provide supporting information. You can disable prompting to facilitate CLI scripting. The default value is `enabled`.
`show who`	Displays a list of users who are currently logged in. For more information, see "User Status" on page 37.
`show history`	This command brings up the history of the last 10 commands.
`traceroute`	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **`traceroute`** *<host name>*| *<IP address>* [*<max-hops (1-32)>* [*delay*]] Where *IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-32 devices), and *delay* (optional) is the number of seconds for wait for the response. The DNS parameters must be configured if specifying hostnames.

Command Line Interface Shortcuts

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same mode. For example, consider the following full command and a valid abbreviation:

```
RS G8000(config)# stack master-ip-interface address <IP address>
```

or

```
RS G8000 (config)# st m a <IP address>
```

Tab Completion

By entering the first characters of a command at any prompt and pressing <*Tab*>, if only one command fits the input text when <*Tab*> is pressed, that command is supplied on the command line, waiting to be entered.

For example, if you enter the following partial command, followed by the tab key, the system attempts to complete the command:

```
RS G8000(config)# stack m <Tab>

RS G8000(config)# stack master-ip-interface
```

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the switch. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- **user**: Interaction with the switch is completely passive—nothing can be changed on the switch. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- **oper**: Interaction with the switch is completely passive—nothing can be changed on the G8000. Users can display information that has no security or privacy implications, such as switch statistics and current operational state information. Users who have an ID with oper privileges can make operational changes, such as running operational-level commands to disable an interface.
- **admin**: Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the switch. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique user names and passwords. After you connect to the switch via local Telnet, remote Telnet, SSH, or Browser Based Interface (BBI) session, you must enter a password. The default user names/password for each access level are listed in the following table.

NOTE – It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies.

Table 1-3 User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	`user`
Operator	Interaction with the switch is completely passive—nothing can be changed on the G8000. Users can display information that has no security or privacy implications, such as switch statistics and current operational state information. Users who have an ID with oper privileges can make operational changes, such as running operational-level commands to disable an interface.	
Administrator	The superuser Administrator has complete access to all command modes, information, and configuration commands on the switch, including the ability to change both the user and administrator passwords.	`admin`

Idle Timeout

By default, the switch will disconnect your Telnet session after five minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes:

`system idle` *<1-60>*

Command mode: Global Configuration

CHAPTER 2
Information Commands

This chapter explains how to use the Command Line Interface (CLI) to display switch information.

Table 2-1 General Information commands

Command Syntax and Usage
`show interface information` Displays port status information, including: ■ Port name, alias, and number ■ Whether the port uses VLAN Tagging or not ■ Port VLAN ID (PVID) ■ VLAN membership To view an example of the command output, see page 65. **Command mode:** All
`show interface link` Displays configuration information about each port, including: ■ Port name, alias, and number ■ Port speed ■ Duplex mode (half, full, or auto) ■ Flow control for transmit and receive (no or yes) ■ Link status (up, down, or disabled) **Command mode:** All To view an example of the command output, see page 66.

Table 2-1 General Information commands

Command Syntax and Usage
`show transceivers` Displays information about SFP/SFP+ transceivers. To view an example of the command output, see page 67. **Command mode:** All
`show information-dump` Dumps all switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Note**: This document does not contain an example of an information-dump because of space limitations. **Command mode:** All

System Information

The information provided by each command option is briefly described in Table 2-2, with links to more detailed information.

Table 2-2 System Information Commands

Command Syntax and Usage
`show sys-info` Displays system information, including: ■ System date and time ■ Switch up-time ■ Reason for last boot ■ MAC address ■ PCBA Part Number ■ Serial Number ■ Manufacturing Date ■ Temperature sensor information ■ Fan speed RPMs ■ Status of each power supply **Command mode:** All To view an example of the command output, see page 36.
`show logging messages` Displays most recent syslog messages. To view an example of the command output, see page 37. **Command mode:** All
`clear logging` Clears syslog messages. **Command mode:** All except User EXEC
`show access user` Displays configured user names and their status. **Command mode:** All except User EXEC To view an example of the command output, see page 37.
`show access user uid` *<1-10>* Displays details for the selected user ID, including name and class of service. **Command mode:** All except User EXEC

SNMPv3 System Information

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 framework by supporting the following:

- A new SNMP message format
- Security for messages
- Access control
- Remote configuration of SNMP parameters

See RFC2271 to RFC2276 for details about SNMPv3 architecture.

Table 2-3 SNMPv3 Commands

Command Syntax and Usage

`show snmp-server v3 user`

Displays User Security Model (USM) table information. The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. To view an example of the command output, see page 27.

Command mode: All

`show snmp-server v3 view`

Displays information about view, subtrees, mask and type of view. The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons. To view an example of the command output, see page 27.

Command mode: All

`show snmp-server v3 access`

Displays View-based Access Control information. The access control subsystem provides authorization services. The `vacmAccessTable` maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view. The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view, and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification. To view an example of the command output, see page 29.

Command mode: All

Table 2-3 SNMPv3 Commands

Command Syntax and Usage
`show snmp-server v3 group` Displays information about the group that includes the security model, user name, and group name. A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name. To view an example of the command output, see page 31. **Command mode:** All
`show snmp-server v3 community` Displays the community table information stored in the SNMP engine. To view an example of the command output, see page 31. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (noAuthnoPriv, authNoPriv, or authPriv). To view an example of the command output, see page 32. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the current target parameters table information. To view an example of the command output, see page 33. **Command mode:** All
`show snmp-server v3 target-parameters` *<1-16>* Displays the Target parameters table index for the selected parameter. To view an example of the command output, see page 33. **Command mode:** All
`show snmp-server v3 notify` Displays the notify table information. To view an example of the command output, see page 34. **Command mode:** All
`show snmp-server v3` Displays all the SNMPv3 information. To view an example of the command output, see page 35. **Command mode:** All

SNMPv3 User-based Security Model User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. The USM uses a defined set of user identities that are displayed in the USM user table. The following command displays SNMPv3 user information:

`show snmp-server v3 user` *<1-16>*

Command mode: All

The USM makes use of a defined set of user identities displayed in the USM user table.
The USM user table contains information, including:

- The user name
- A security name in the form of a string whose format is independent of the Security Model
- An authentication protocol, which indicates that the messages sent on behalf of the user can be authenticated
- the privacy protocol _

```
User Name                      Protocol
----------------------------- ------------------------------
adminmd5                       HMAC_MD5   DES PRIVACY
adminsha                       HMAC_SHA   DES PRIVACY
v1v2only                       No Auth    NO PRIVACY
```

Table 2-4 USM User Table Information Parameters

Field	Description
`User Name`	This is a string that represents the name of the user that you can use to access the switch.
`Protocol`	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. The switch supports DES algorithm for privacy. The switch also supports the MD5 and HMAC-SHA Authentication algorithms.

SNMPv3 View Table Information

Each user can control and restrict the access allowed to a group to a subset of the management information in the management domain that the group can access within each context, by specifying the group's rights in terms of a particular MIB view for security reasons.

The following command displays the SNMPv3 View Table.

`show snmp-server v3 view`

Command mode: All

```
View Name            Subtree                        Mask    Type
------------------   ---------------------------    -----   --------
iso                  1                                      Included

v1v2only             1                                      Included

v1v2only             1.3.6.1.6.3.15                         Excluded

v1v2only             1.3.6.1.6.3.16                         Excluded

v1v2only             1.3.6.1.6.3.18                         Excluded
```

Table 2-5 SNMPv3 View Table Information Parameters

Field	Description
`View Name`	Displays the name of the view.
`Subtree`	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
`Mask`	Displays the bit mask.
`Type`	Displays whether a family of view subtrees is included or excluded from the MIB view.

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

The `vacmAccessTable` maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use to check the access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following command displays SNMPv3 access information:

`show snmp-server v3 access`

Command mode: All

```
Group Name  Model    Level        ReadV      WriteV     Notify
---------- ------- ------------ ----------- ---------- ----------
v1v2grp    snmpv1   noAuthNoPriv  iso        iso        v1v2only
admingrp   usm      AuthPriv      iso        iso        iso
```

Table 2-6 SNMPv3 Access Table Information

Field	Description
`Group Name`	Displays the name of group.
`Model`	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
`Level`	Displays the minimum level of security required to gain rights of access. For example, `noAuthNoPriv`, `authNoPriv`, or `auth-Priv.`
`ReadV`	Displays the MIB view to which this entry authorizes the read access.
`WriteV`	Displays the MIB view to which this entry authorizes the write access.
`NotifyV`	Displays the Notify view to which this entry authorizes the notify access.

SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following command displays SNMPv3 group information:

`show snmp-server v3 group`

Command mode: All

```
Sec Model   User Name                            Group Name
---------- ------------------------------  --------------------
snmpv1      v1v2only                          v1v2grp
usm         adminmd5                          admingrp
usm         adminsha                          admingrp
```

Table 2-7 SNMPv3 Group Table Information Parameters

Field	Description
`Sec Model`	Displays the security model used, which is any one of: USM, SNMPv1 and SNMPv2.
`User Name`	Displays the User Name for the group.
`Group Name`	Displays the access name of the group.

SNMPv3 Community Table Information

The following command displays SNMPv3 community information stored in the SNMP engine:

show snmp-server v3 community

Command mode: All

```
Index      Name       User Name            Tag
---------- ---------- -------------------- ---------
trap1      public     v1v2only             v1v2trap
```

Table 2-8 SNMPv3 Community Table Parameters

Field	Description
`Index`	Displays the unique index value of a row in this table.
`Name`	Displays the community string, which represents the configuration.
`User Name`	Displays the User Security Model (USM) user name.
`Tag`	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

`show snmp-server v3 target-address`

Command mode: All

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

```
Name          Transport Addr    Taglist    Params
----------    ---------------   -------    ----------
trap1         47.81.25.66       v1v2trap   v1v2param
```

Table 2-9 SNMPv3 Target Address Table Information Parameters

Field	Description
`Name`	Displays the locally arbitrary, but unique identifier associated with this `snmpTargetAddrEntry`.
`Transport Addr`	Displays the transport addresses.
`Taglist`	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
`Params`	The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

`show snmp-server v3 target-parameters`

Command mode: All

```
Name            MP Model   User Name          Sec Model    Sec Level
--------------- --------   --------------     ---------    ---------
v1v2param      snmpv2c    v1v2only         snmpv1       noAuthNoPriv
```

Table 2-10 SNMPv3 Target Parameters Table Information

Field	Description
`Name`	Displays the locally arbitrary, but unique identifier associated with this `snmpTargetParamsEntry`.
`MP Model`	Displays the Message Processing Model used when generating SNMP messages using this entry.
`User Name`	Displays the `securityName`, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
`Sec Model`	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an `inconsistentValue` error if an attempt is made to set this variable to a value for a security model which the system does not support.
`Sec Level`	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Target Parameters Table Index Information

The following command displays SNMPv3 target parameters index information:

`show snmp-server v3 target-parameters` *<1-16>*

Command mode: All

```
name , mpmodel snmpv3
    uname , model usm ,level noauthnoPriv
```

Table 2-11 SNMPv3 Target Parameters Table Index Information

Field	Description
`Name`	Displays the locally arbitrary, but unique identifier associated with this `snmpTargeParamsEntry`.
`mpmodel`	Displays the Message Processing Model used when generating SNMP messages using this entry.
`uname`	Displays the `securityName`, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
`model usm`	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an `inconsistentValue`error if an attempt is made to set this variable to a value for a security model which the system does not support.
`level`	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify Table:

`show snmp-server v3 notify`

Command mode: All

```
Name                  Tag
--------------------  --------------------
v1v2trap              v1v2trap
```

Table 2-12 SNMPv3 Notify Table Information

Field	Description
`Name`	The locally arbitrary, but unique identifier associated with this `snmpNotifyEntry`.
`Tag`	This represents a single tag value which is used to select entries in the `snmpTargetAddrTable`. Any entry in the `snmpTargetAddrTable` that contains a tag value equal to the value of this entry is selected. If this entry contains a value of zero length, no entries are selected.

SNMPv3 Dump Information

The following command displays SNMPv3 information:

show snmp-server v3

Command mode: All_

```
EngineId: 80.00.08.1c.04.46.53

usmUser Table:
User Name                     Protocol
----------------------------  ------------------------------
adminmd5                      HMAC_MD5   DES PRIVACY
adminsha                      HMAC_SHA   DES PRIVACY
v1v2only                      No Auth    NO PRIVACY

vacmAccess Table:
Group Name     Model      Level         ReadV        WriteV       Notify
----------     -------   ------------   -----------  ----------   ----------
v1v2grp        snmpv1    noAuthNoPriv   iso          iso          v1v2only
admingrp       usm       AuthPriv       iso          iso          iso

vacmViewTreeFamily Table:
View Name            Subtree                          Mask             Type
-------------------- -------------------------------- --------------   ------
iso                 1                                                Included

v1v2only            1                                                Included

v1v2only            1.3.6.1.6.3.15                                   Excluded

v1v2only            1.3.6.1.6.3.16                                   Excluded


v1v2only            1.3.6.1.6.3.18                                   Excluded
...
```

General System Information

The following command displays system information:

`show sys-info`

Command mode: All

```
Blade Network Technologies Rack Switch G8000

System Information at
 Sun Jan 15 23:56:24 2009
 Switch has been up for 0 day, 0 hour, 19 minutes and 31 seconds
Last boot:(power cycle)

MAC address: 00:18:b1:8a:36:00    IP (If 1) address: 172.24.1.70
Revision: 8
Switch Serial No: US38200028
Spare Part No: BAC-00017-00
Manufacturing date: 08/20
Software Version 6.0.1 (FLASH image2), active configuration.

Fans are in Forward AirFlow, Warning at 55 C and Recover at 80 C

Temperature Sensor 1:   32.0 C
Temperature Sensor 2:   38.0 C
Temperature Sensor 3: --.-
Temperature Sensor 4:   31.0 C

Speed of Fan 1: 0 RPM
Speed of Fan 2: 0 RPM
Speed of Fan 3: 0 RPM
Speed of Fan 4: 4224 RPM
Speed of Fan 5: 6272 RPM

State of Power Supply 1:   On
State of Power Supply 2:   Off
```

NOTE – The temperature sensor display is only visible if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

System information includes:

- Switch up-time
- Reason for last boot
- MAC address
- Software version
- PCBA part number
- FAB number
- Serial number
- Manufacturing date
- Hardware revision
- Board revision
- CPLD firmware version
- Temperature sensor information
- Fan speed RPMs
- Power supply status

Show Syslog Messages

The following command displays system log messages:

`show logging messages`

Command mode: All

```
Jan 26 2008 18:03:27 RS G8000:CLI-ALERT:User (admin) logged in on console
Jan 26 2008 18:07:32 RS G8000:CFA-NOTICE:system: link up on port 2:2
Jan 26 2008 18:11:12 RS G8000:SYSTEM-CRITICAL:Warning: Fan Failure
```

User Status

The following command displays the status of configured user names.

show access user

Command mode: All except User EXEC

```
Usernames:
  admin - Always Enabled   - online  1 session.
  user  - enabled          - offline
  oper  - disabled         - offline
```

The following global command displays information about users who are logged in:

show who

Command mode: All except User EXEC

```
Line User          Peer-Address          COS   Login-Time Last-Cmd
==== ============= ===================== ===== ========== =======
tel  admin         10.10.10.224:1735     admin 19:8:52    show who
```

The following information is provided for each current user:

- Connection type
- User name
- User IP address
- Class of Service
- Time of login
- Last command issued by the user

Stacking Information

Table 2-13 lists the Stacking Information commands.

Table 2-13 Stacking Information commands

Command Syntax and Usage
`show stack switch` Displays information about each switch in the stack, including: ■ Configured Switch Number (csnum) ■ Assigned Switch Number (asnum) ■ MAC address ■ Stacking state **Command mode:** All except user EXEC
`show stack link` Displays link information for each switch in the stack. **Command mode:** All except user EXEC
`show stack name` Displays the configured name of the stack. **Command mode:** All except user EXEC
`show stack version` Displays the firmware version number for the selected switch. **Command mode:** All except user EXEC
`show stack master-ip-interface` Displays the IP address and gateway of the Master Switch Interface. **Command mode:** All except user EXEC
`show stack backup-ip-interface` Displays the IP address and gateway of the Backup Switch Interface. **Command mode:** All except user EXEC
`show stack path-map` [<*csnum 1-6*>] Displays the Stacking packet path map that shows how the stack switches are connected. **Command mode:** All except user EXEC
`show stack push-status` Displays the status of the most recent firmware and configuration file push from the master to member switches. **Command mode:** All except user EXEC

Table 2-13 Stacking Information commands

Command Syntax and Usage
`show stack dynamic` Displays all stacking information. **Command mode:** All except user EXEC

Show Stacking Switch Information

The following command displays Stacking switch information:

show stack switch

Command mode: All

```
Stack name: Stack1
Local switch is the master.

Local switch:
   csnum              - 1
   MAC                - 00:22:00:ac:bd:00
   Switch Type        - 9
   Chassis Type       - 99
   Switch Mode (cfg)  - Master
   Priority           - 225
   Stack MAC          - 00:22:00:ac:bd:1f

Master switch:
   csnum              - 1
   MAC                - 00:22:00:ac:bd:00

Backup switch:
   csnum              - 3
   MAC                - 00:00:60:10:00:00

Configured Switches:
-------------------------------------
csnum           MAC          asnum
-------------------------------------
 C1     00:22:00:ac:bd:00    A1
 C2     00:00:00:00:00:00
 C3     00:00:60:10:00:00    A2

Attached Switches in Stack:
---------------------------------------------
asnum           MAC          csnum  State
---------------------------------------------
 A1     00:22:00:ac:bd:00     C1    IN_STACK
 A2     00:00:60:10:00:00     C3    IN_STACK
```

Stack switch information includes the following:

- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Backup
- Configured switch numbers and their associate assigned switch numbers
- Assigned switch numbers and their associate configured switch numbers

Layer 2 Information

Table 2-14 contains a summary of Layer 2 general information commands. The sections after the table describe detailed Layer 2 information commands.

Table 2-14 Layer 2 General Information Commands

Command Syntax and Usage
`show dot1x` Displays current global 802.1X parameters. To view an example of the command output, see page 50. **Command mode:** All
`show dot1x information` Displays 802.1X information. **Command mode:** All
`show portchannel information` When trunk groups are configured, you can view the state of each port in the various trunk groups. To view an example of the command output, see page 52. **Command mode:** All
`show vlan` *<1-4094>* Displays VLAN configuration information for all configured VLANs, including: ■ VLAN Number ■ VLAN Name ■ Status ■ Jumbo Frame usage ■ Port membership of the VLAN **Command mode:** All
`show layer2 information` Dumps all Layer 2 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

Forwarding Database Information

The Forwarding Database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

NOTE – The master Forwarding Database supports up to 16K MAC address entries.

Table 2-15 FDB Information Commands

Command Syntax and Usage
`show mac-address-table` Displays all entries in the Forwarding Database. To view an example of the command output, see page 45. **Command mode:** All
`show mac-address-table address` *<MAC address>* Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56` You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456` **Command mode:** All
`show mac-address-table interface port` *<port number>* Displays all FDB entries for a particular port. **Command mode:** All
`show mac-address-table portchannel` *<trunk group number>* Displays all FDB entries for a particular trunk group. **Command mode:** All
`show mac-address-table state {forward|trunk|unknown}` Displays all FDB entries for a particular state. **Command mode:** All
`show mac-address-table vlan` *<1-4094>* Displays all FDB entries on a single VLAN. **Command mode:** All

Show All FDB Information

The following command displays Forwarding Database information:

`show mac-address-table`

Command mode: All

```
Mac address Aging Time: 300

    MAC address      VLAN  Port  Trnk  State
 -----------------   ----  ----  ----  -----
 00:01:02:03:04:05      1    14          FWD
 00:03:47:0a:54:19      1    14          FWD
 00:07:e9:39:07:8a      1    14          FWD
 00:08:74:a9:1d:e9      1    14          FWD
 00:09:6b:ca:1a:be      1    14          FWD
 00:09:97:16:69:00      1    14          FWD
 00:0e:0c:b3:65:4d      1    14          FWD
 00:0f:fe:2d:f5:39      1    14          FWD
 00:0f:fe:af:b7:6e      1    14          FWD
 00:0f:fe:b0:62:0e      1    14          FWD
 00:0f:fe:b3:de:7e      1    14          FWD
 00:11:11:e3:70:50      1    14          FWD
 00:11:25:c3:2a:3c      1    14          FWD
 00:13:0a:4f:7c:90      1    14          FWD
 00:15:ed:00:00:00      1    14          FWD
 00:16:17:7c:e0:c0      1    14          FWD
 00:16:17:81:10:a9      1    14          FWD
 00:16:17:81:13:b7      1    14          FWD
```

An address that is in the forwarding (`FWD`) state has been learned by the switch on a port (not a portchannel/trunk group). Addresses in the trunking (`TRK`) state have been learned through a portchannel/trunk group. If the state of the port is listed as unknown (`UNK`), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated, although ports which reference the address as a destination will be listed under “Reference ports.”

Clearing Entries From the Forwarding Database

To delete a MAC address from the forwarding database (FDB) or to clear the entire FDB, see “Forwarding Database Maintenance” on page 189.

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the switch.

Table 2-16 LACP Information Commands

Command Syntax and Usage
`show lacp aggregator {`*<port number>***`}`** Displays detailed information about the LACP aggregator used by the selected port. **Command mode:** All
`show lacp` Displays the configured global LACP settings. **Command mode:** All
`show lacp information` Displays a summary of LACP information. To view an example of the command output, see page 47. **Command mode:** All

Link Aggregation Control Protocol

The following command displays LACP information:

`show lacp information`

Command mode: All

```
port  lacp    adminKey  operKey   selected    prio      attached
                                                    aggr     trunk    status
----- -----   -------   -------   -------    ----     ---      -----    ----
1     off     0         0         n           32768     --       --        --
2     off     0         0         n           32768     --       --        --
3     off     0         0         n           32768     --       --        --
4     off     0         0         n           32768     --       --        --
5     off     0         0         n           32768     --       --        --
...
```

LACP dump includes the following information for each port on the switch:

- lacp
  Displays the port’s LACP mode (active, passive, or off)
- adminkey
  Displays the value of the port’s *adminkey*.
- operkey
  Shows the value of the port’s operational key.

- selected
  Indicates whether the port has been selected to be part of a Link Aggregation Group.
- prio
  Shows the value of the port priority.
- attached aggr
  Displays the aggregator associated with each port.
- trunk
  This value represents the LACP trunk group number.
- status
  This value represents the status of the port in LACP (active or down).

Layer 2 Failover Information

Table 2-17 Layer 2 Failover Information commands

Command Syntax and Usage
`show failover trigger` *<1-8>* Displays detailed information about the selected Layer 2 Failover trigger. **Command mode:** All
`show failover` Displays a summary of Layer 2 Failover information. **Command mode:** All For details, see page 47.

Layer 2 Failover information

The following command displays Layer 2 Failover information:

show failover

Command mode: All

```
Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member       Status
---------    -----------
trunk 1
 2:2        Operational
 2:3        Operational

Control State: Auto Disabled
Member       Status
---------    -----------
 1:1        Operational
 1:2        Operational
 1:3        Operational
 1:4        Operational
...
```

The Layer 2 Failover trigger information includes the following:

- Monitor status (enabled or disabled)
- Trigger limit
- Monitor state (up or down)
- Monitor members and status of each member (operational or failed)
- Control members and status of each member (operational or failed)

802.1X Information

The following command displays 802.1X information:

`show dot1x`

Command mode: All

```
System capability : Authenticator
System status     : enabled
Protocol version  : 1
Guest VLAN status : disabled
Guest VLAN        : none
                                 Authenticator    Backend   Assigned
Port    Auth Mode    Auth Status     PAE State      Auth State   VLAN
-----  ------------  ------------  --------------  ---------- ------
*1:1   force-auth    unauthorized  initialize      initialize   none
*1:2   force-auth    unauthorized  initialize      initialize   none
*1:3   force-auth    unauthorized  initialize      initialize   none
*1:4   force-auth    unauthorized  initialize      initialize   none
*1:5   force-auth    unauthorized  initialize      initialize   none
*1:6   force-auth    unauthorized  initialize      initialize   none
*1:7   force-auth    unauthorized  initialize      initialize   none
*1:8   force-auth    unauthorized  initialize      initialize   none
*1:9   force-auth    unauthorized  initialize      initialize   none
*1:10  force-auth    unauthorized  initialize      initialize   none
*1:11  force-auth    unauthorized  initialize      initialize   none
*1:12  force-auth    unauthorized  initialize      initialize   none
...
------------------------------------------------------------------
* - Port down or disabled
```

The following table describes the IEEE 802.1X parameters.

Table 2-18 802.1X Parameter Descriptions (/info/l2/8021x)

Parameter	Description
Port	Displays each port's alias.
`Auth Mode`	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: ■ force-unauth ■ auto ■ force-auth
`Auth Status`	Displays the current authorization status of the port, either authorized or unauthorized.

Table 2-18 802.1X Parameter Descriptions (Continued)(/info/l2/8021x)

Parameter	Description
`Authenticator PAE State`	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: ■ initialize ■ disconnected ■ connecting ■ authenticating ■ authenticated ■ aborting ■ held ■ forceAuth
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: ■ initialize ■ request ■ response ■ success ■ fail ■ timeout ■ idle
Assigned VLAN	Displays the VLAN assigned to the port, if applicable.

Trunk Group Information

Use these commands to display information about trunk groups (portchannels).

Table 2-19 Portchannel information commands

Command Syntax and Usage
`show portchannel` *<trunk number>* Displays information about the selected static trunk group. **Command mode:** All
`show portchannel` *<LACP trunk number>* Displays information about the selected LACP trunk group. **Command mode:** All
`show portchannel information` Displays a summary of trunk group information. To view an example of the command output, see page 52. **Command mode:** All

Trunk Group

The following command displays Trunk Group information:

`show portchannel information`

Command mode: All

```
PortChannel group 1, Enabled
Protocol - Static
Port State:
  2:2: detached
  2:3: detached
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

VLAN Information

The following command displays VLAN information:

`show vlan`

Command mode: All

```
VLAN                Name                Status            Ports
----  --------------------------------  ------  -------------------------
1     Default VLAN                      ena     1:1-1:50 2:1-2:50 3:1-3:50
                                                4:1-4:50 5:1-5:50 6:1-6:50
20    VLAN 20                           ena     empty
30    VLAN 30                           ena     empty
4090  STK VLAN                          ena     1:51 1:52 2:51 2:52 3:51 3:52
                                                4:51 4:52 5:51 5:52 6:51 6:52
```

This information display includes all configured VLANs and all member ports.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN.
- Trunk group (portchannel) membership of the VLAN

Layer 3 Information

The following table lists general Layer 3 information commands. The following sections contain more detailed commands

Table 2-20 Layer 3 Information Commands

Command Syntax and Usage
`show layer3 information` Dumps all Layer 3 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

The following command displays Layer 3 information:

`show layer3 information`

Command mode: All

```
Interface information:
   1: 10.1.1.1          255.255.0.0         10.1.1.255,vlan1, up

Default gateway information:
  10.1.1.2, enabled,  active

Master switch IP interface configured through DHCP
MAC address:        00:22:00:ac:bd:1f
IP address:         127.31.37.158
Subnet mask:        255.255.0.0
Default gateway:    127.31.1.1
DHCP Server:        127.31.35.1
Lease Obtained:     11:35:44 Mon Aug  3, 2009
Lease Expires:      14:31:40 Mon Aug 10, 2009

Current ARP configuration:
rearp 5
ARP cache information:

IP Address       Flags     Hardware Address    Interface
--------------   ------    -----------------   ---------
10.1.1.1                   00:15:40:07:20:42    1

Route table information:
Status code: * - best
Destination      Mask            Gateway          Type      Tag        Metr  If
---------------  --------------- ---------------  ---------- ---------- ---- ---
* 10.1.1.0        255.255.255.0    0.0.0.0         direct     fixed          1
* 10.1.1.1        255.255.255.255  10.1.1.1        local      addr       0    1
* 10.1.1.255      255.255.255.255  10.1.1.255      bcast      bcast      0    1
```

ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags, VLAN and port for the address, and port referencing information.

Table 2-21 ARP Information Commands

Command Syntax and Usage
`show ip arp find` *<IP address>* Displays a single ARP entry by IP address. **Command mode:** All
`show ip arp vlan` *<1-4094>* Displays all ARP entries learned on the selected VLAN. **Command mode:** All
`show ip arp interface port` *<port number>* Displays ARP entries learned on the selected port. **Command mode:** All
`show ip arp reply` Shows the list of IP addresses that the switch will respond to for ARP requests. **Command mode** All
`show ip arp` Displays information about all ARP entries, including: ■ Re-ARP interval ■ Static ARP entries ■ IP address and MAC address of each entry ■ Address mapping ■ The interface to which the address belongs **Command mode:** All To view an example of the command output, see page 56.

Show All ARP Entry Information

The following command displays ARP information:

`show ip arp`

Command mode: All

```
Current ARP configuration:
 rearp 5

Current static ARP:
ip               mac                  interface
--------------   -----------------    ---------


IP Address       Flags     Hardware Address    Interface
--------------   ------    -----------------   ---------
127.20.1.1                 00:15:40:07:20:42    1
127.20.254.21    P         00:22:00:4d:b9:00    1
```

IGMP Multicast Group Information

Table 2-22 IGMP Multicast Group Information Commands

Command Syntax and Usage
`show ip igmp groups address` *<IP address>* Displays IGMP multicast group information by the group's IP address. **Command mode:** All
`show ip igmp groups interface port` *<port number>* Displays all IGMP multicast groups on a single port. **Command mode:** All
`show ip igmp groups portchannel` *<trunk number>* Displays all IGMP multicast groups on a selected trunk group. Note that portchannel 1-52 indicates static trunks, and portchannel 53-104 indicate LACP trunks. **Command mode:** All
`show ip igmp groups vlan` *<1-4094>* Displays all IGMP multicast groups on a selected VLAN. **Command mode:** All
`show ip igmp groups` Displays information for all multicast groups. **Command mode:** All
`show ip igmp mrouter information` Displays IGMP Multicast Router information. **Command mode:** All
`show ip igmp mrouter vlan` *<1-4094>* Displays IGMP multicast routers for the selected VLAN. **Command mode:** All

IGMP Group Information

The following command displays IGMP Group information:

`show ip igmp groups`

Command mode: All

```
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
     Group           VLAN     Port    Version    Expires
---------------- -------- ------ --------    -------
226.0.0.0        1        1:18    V2         3:19
226.0.0.1        1        1:18    V2         3:19
226.0.0.2        1        1:18    V2         3:19
226.0.0.3        1        1:18    V2         3:19
226.0.0.4        1        1:18    V2         3:19
```

IGMP Group information includes:

- IGMP Group address
- VLAN and port
- IGMP version
- Expiration timer value

IGMP Multicast Router Information

The following command displays multicast router information:

`show ip igmp mrouter information`

Command mode: All

```
SrcIP                VLAN      Port      Version    Expires    MRT
------------------ ------    ------    --------   -------    ------
10.10.254.10        1        5:44       V2       3:59      10
```

IGMP Mrouter information includes:

- Source IP address
- VLAN number
- Port number
- IGMP version
- Expiration time

IP Information

The following command displays Layer 3 IP information:

`show ip information`

Command mode: All

```
Interface information:

1: 10.200.30.3  255.255.255.0   3.3.3.255,     vlan 1, up

Default gateway information: metric strict
  1: 10.200.1.1,     vlan any,  up

Master switch IP interface configured through DHCP
MAC address:        00:22:00:ac:bd:1f
IP address:         12.31.37.158
Subnet mask:        255.255.0.0
Default gateway:    12.31.1.1
DHCP Server:        12.31.35.1
Lease Obtained:     11:00:18 Mon Aug 10, 2009
Lease Expires:      20:12:37 Tue Aug 11, 2009
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask/prefix, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status.
- Stacking Master Interface information.

QoS Information

The following command displays 802.1p information:

`show qos transmit-queue information`

Command mode: All

```
Current priority to COS queue information:
Priority  COSq  Weight
--------  ----  ------
    0       0      1
    1       0      1
    2       0      1
    3       0      1
    4       0      1
    5       0      1
    6       0      1
    7       1      4

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
1:1        0       0      1
1:2        0       0      1
...

2:1        0       0      1
2:2        0       0      1
2:3        0       0      1
2:4        0       0      1
...
```

Table 2-23 describes the IEEE 802.1p priority-to-COS queue information.

Table 2-23 802.1p Priority-to-COS Queue parameter descriptions

Parameter	Description
`Priority`	Displays the 802.1p Priority level.
`COSq`	Displays the Class of Service queue.
`Weight`	Displays the scheduling weight of the COS queue.

Table 2-24 describes the IEEE 802.1p port priority information.

Table 2-24 802.1p Port Priority parameter descriptions

Parameter	Description
`Port`	Displays the port alias.
`Priority`	Displays the 802.1p Priority level.
`COSq`	Displays the Class of Service queue.
`Weight`	Displays the scheduling weight.

QoS DSCP Information

The following command displays DSCP information:

`show qos dscp`

Command mode: All except User EXEC

```
Current DSCP Mapping Configuration:  OFF
  DSCP    New 802.1p Prio
--------  ---------------
    0          0
    1          0
    2          0
    3          0
    4          0
    5          0
    6          0
    7          0
    8          1
    9          0
   10          1
   11          0
   12          1
...
```

Table 2-25 describes QoS DSCP information parameters.

Table 2-25 DSCP information

Field	Description
`DSCP`	Displays the DiffServ Code Point (DSCP) number.
`New 802.1p Priority`	Displays the new 802.1p Priority level.

Access Control List Information

Access Control List Information

The following command displays Access Control List (ACL) information:

`show access-control`

Command mode: All

```
Current ACL information:
------------------------
  Filter 2 profile:
   Ethernet
     - VID        : 2/0xfff
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Actions        : Permit
  No ACL groups configured.
```

Access Control List (ACL) information includes configuration settings for each ACL and ACL Group.

Table 2-26 ACL Parameter Descriptions

Parameter	Description
`Filter x profile`	Indicates the ACL number.
`Meter`	Displays the ACL meter parameters.
`Re-Mark`	Displays the ACL re-mark parameters.
`Actions`	Displays the configured action for the ACL.

Port Information

The following command displays port information:

`show interface information`

Command mode: All except User EXEC

```
Alias Port Tag    Type    PVID       NAME                  VLAN(s)
----- ---- --- ---------- ----- -------------- ---------------------
1:1   65    n  External      1* External1:1    1
1:2   66    n  External      1* External1:2    1
1:3   67    n  External      1* External1:3    1
1:4   68    n  External      1* External1:4    1
1:5   69    n  External      1* External1:5    1
1:6   70    n  External      1* External1:6    1
1:7   71    n  External      1* External1:7    1
1:8   72    n  External      1* External1:8    1
1:9   73    n  External      1* External1:9    1
1:10  74    n  External      1* External1:10   1
...
# = PVID is tagged.
```

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Port VLAN ID (`PVID`)
- Port name
- VLAN membership

Interface Link Information

The following command displays port link status for each port on the switch:

`show interface link`

Command mode: All except User EXEC

```
RS G8000(config)# show interface link
-----------------------------------------------------------------------
Alias    Port   Speed    Duplex     Flow Ctrl      Link
-----    ----   -----   --------  --TX-----RX--   ------
1:1       65      any      any     yes     yes      down
1:2       66      any      any     yes     yes      down
1:3       67      any      any     yes     yes      down
1:4       68      any      any     yes     yes      down
1:5       69      any      any     yes     yes      down
1:6       70      any      any     yes     yes      down
1:7       71      any      any     yes     yes      down
1:8       72      any      any     yes     yes      down
1:9       73      any      any     yes     yes      down
1:10      74      any      any     yes     yes      down
1:11      75      any      any     yes     yes      down
1:12      76      any      any     yes     yes      down
1:13      77      any      any     yes     yes      down
1:14      78      any      any     yes     yes      down
1:15      79      any      any     yes     yes      down
1:16      80      any      any     yes     yes      down
1:17      81      any      any     yes     yes      down
1:18      82      any      any     yes     yes      down
1:19      83      any      any     yes     yes      down
1:20      84      any      any     yes     yes      down
...
```

Port link information includes the following:

- Port alias and number
- Port speed (10, 100, 1000, or any)
- Duplex mode (half, full, or any)
- Flow control for transmit and receive (no or yes)
- Link status (up, down, or disabled)

Interface Transceivers

The following command displays transceivers used on the switch.

`show transceivers`

Command mode: All except User EXEC

```
Modules:
Switch    IO Module         Type         Part Number             Serial
------   ------------   ------------   ----------------      ----------------
1        Front module    Not inserted
1        Rear module     CX4              BAC-00027-00            CH4825008X
```

Information Dump

The following command dumps switch information:

`show information-dump`

Command mode: All

Use the dump command to dump all switch information available (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

CHAPTER 3
Statistics Commands

You can view switch performance statistics in the user, operator, and administrator command modes. This chapter discusses how to use the ISCLI to display switch statistics.

Table 3-1 Statistics Commands

Command Syntax and Usage

`show snmp-server`

Displays the current SNMP configuration parameters. To view an example of the command output, see page 94.

Command mode: All

`show snmp-server counters`

Displays SNMP statistics. To view an example of the command output, see page 94.

Command mode: All

`clear ntp`

Clears Network Time Protocol (NTP) statistics.

Command mode: All except User EXEC

`clear ntp primary-server`

Clears statistics for the primary NTP server.

Command mode: All except User EXEC

`clear ntp secondary-server`

Clears statistics for the secondary NTP server.

Command mode: All except User EXEC

`show counters`

Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. To view an example of the command output, see page 98.

Command mode: All

Port Statistics

These commands display traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

Table 3-2 Port Statistics Commands

Command Syntax and Usage
`show interface port {`*<port number, or range of ports>*`} bridging-counters` Displays bridging ("dot1") statistics for the port. To view an example of the command output, see page 75. **Command mode:** All
`show interface port {`*<port number, or range of ports>*`} dot1x` Displays IEEE 802.1X statistics for the port. To view an example of the command output, see page 73. **Command mode:** All
`show interface port {`*<port number, or range of ports>*`} ethernet-counters` Displays Ethernet ("dot3") statistics for the port. To view an example of the command output, see page 76. **Command mode:** All
`show interface port {`*<port number, or range of ports>*`} interface-counters` Displays interface statistics for the port. To view an example of the command output, see page 78. **Command mode:** All
`show interface port {`*<port number, or range of ports>*`} ip-counters` Displays IP statistics for the port. To view an example of the command output, see page 81. **Command mode:** All
`show interface port {`*<port number, or range of ports>*`} lacp counters` Displays Link Aggregation Control Protocol (LACP) statistics for the port. To view an example of the command output, see page 82. **Command mode:** All
`show interface port {`*<port number, or range of ports>*`} link-counters` Displays link statistics for the port. To view an example of the command output, see page 83. **Command mode:** All
`clear interface port {`*<port number>*`} counters` Clears all statistics for the port. **Command mode:** All except User EXEC

Table 3-2 Port Statistics Commands

Command Syntax and Usage
`clear interfaces` Clears statistics for all ports. **Command mode:** All except User EXEC
`show interface port {`*<port number, or range of ports>***`} link-counters`** Displays link statistics for the port. To view an example of the command output, see page 83. **Command mode:** All
`clear interface port {`*<port number, or range of ports>***`} counters`** Clears all statistics counters for the selected ports. **Command mode:** Global configuration
`clear interfaces counters` Clears statistics counters for all ports. **Command mode:** All except User EXEC

Port 802.1X Authenticator Statistics

Use the following command to display the 802.1X authenticator statistics for the selected port:

`show interface port {`*<port number, or range of ports>***`} dot1x counters`**

Command mode: All

```
Authenticator Statistics:
--------------------------
eapolFramesRx            = 0
eapolFramesTx            = 0
eapolStartFramesRx       = 0
eapolLogoffFramesRx      = 0
eapolRespIdFramesRx      = 0
eapolRespFramesRx        = 0
eapolReqIdFramesTx       = 0
eapolReqFramesTx         = 0
invalidEapolFramesRx     = 0
eapLengthErrorFramesRx   = 0
lastEapolFrameVersion    = 0
lastEapolFrameSource     = 00:00:00:00:00:00
```

Table 3-3 802.1X Authenticator Statistics of a Port

Statistics	Description
`eapolFramesRx`	Total number of EAPOL frames received.
`eapolFramesTx`	Total number of EAPOL frames transmitted.
`eapolStartFramesRx`	Total number of EAPOL Start frames received.
`eapolLogoffFramesRx`	Total number of EAPOL Logoff frames received.
`eapolRespIdFramesRx`	Total number of EAPOL Response Identity frames received.
`eapolRespFramesRx`	Total number of Response frames received.
`eapolReqIdFramesTx`	Total number of Request Identity frames transmitted.
`eapolReqFramesTx`	Total number of Request frames transmitted.
`invalidEapolFramesRx`	Total number of invalid EAPOL frames received.
`eapLengthErrorFramesRx`	Total number of EAP length error frames received.
`lastEapolFrameVersion`	The protocol version number carried in the most recently received EAPOL frame.
`lastEapolFrameSource`	The source MAC address carried in the most recently received EAPOL frame.

Port 802.1X Authenticator Diagnostics

Use the following command to display the 802.1X authenticator diagnostics for the selected port:

show interface port {*<port alias or number>***} dot1x**

Command mode: All

```
System Status: Disabled

                     Quiet     Tx          Max      Supp      Server    ReAuth    ReAuth
Port   Auth Mode      Period   Period      Req      Timeout   Timeout   Status    Period
----   ---------      ------   ------      ---      ------    -------   ------    ------
G      force-auth     60        30          2        30        30        disabled   3600
1      force-auth     60        30          2        30        30        disabled   3600
--------------------------------------------------------------------------
G - Global port configuration
```

Table 3-4 802.1X Authenticator Diagnostics of a Port

Statistics	Description
`Port`	The port number.
`Auth Mode`	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: ■ `force-unauth` ■ `auto` ■ `force-auth`
`Quiet Period`	Sets the time, in seconds, the authenticator waits before transmitting an EAPRequest/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
`Tx Period`	Sets the time, in seconds, the authenticator waits for an EAP-Response/ Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
`Max Req`	Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.
`Supp Timeout`	Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

Table 3-4 802.1X Authenticator Diagnostics of a Port

Statistics	Description
`Server Timeout`	Sets the time, in seconds, the authenticator waits for a response from the Radius server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of /cfg/sys/radius/timeout (default is three seconds).
`Reauth Status`	Sets the re-authentication status to on or off. The default value is off.
`Reauth Period`	Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

Port Bridging Statistics

Use the following command to display the bridging statistics for the selected port:

```
show interface port {<port number>} bridging-counters
```

Command mode: All

```
Bridging statistics for port 1:
dot1PortInFrames:                    63242584
dot1PortOutFrames:                   63277826
dot1PortInDiscards:                       296
dot1StpPortForwardTransitions:              1
```

Table 3-5 Port Bridging Statistics

Statistics	Description
`dot1PortInFrames`	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
`dot1PortOutFrames`	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
`dot1PortInDiscards`	Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process.
`dot1StpPortForward Transitions`	The number of times this port has transitioned from the Learning state to the Forwarding state.

Port Ethernet Statistics

Use the following command to display the ethernet statistics for the selected port:

show interface port {*<port number, or range of ports>***} ethernet-counters**

Command mode: All

```
Ethernet statistics for port INT1:
dot3StatsAlignmentErrors:                   0
dot3StatsFCSErrors:                         0
dot3StatsSingleCollisionFrames:             0
dot3StatsMultipleCollisionFrames:           0
dot3StatsLateCollisions:                    0
dot3StatsExcessiveCollisions:               0
dot3StatsInternalMacTransmitErrors:        NA
dot3StatsFrameTooLongs:                     0
dot3StatsInternalMacReceiveErrors:          0
```

Table 3-6 Ethernet Statistics for Port

Statistics	Description
`dot3StatsAlignmentErrors`	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `alignmentError` status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
`dot3StatsFCSErrors`	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `frameCheckError` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. **Note**: Values in this statistics counter usually indicate a bad cable.

Table 3-6 Ethernet Statistics for Port

Statistics	Description
dot3StatsSingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrame object.
dot3StatsMultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.
dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 3-6 Ethernet Statistics for Port

Statistics	Description
`dot3StatsFrameTooLongs`	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the `frameTooLong` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
`dot3StatsInternalMacReceiveErrors`	A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsFrameTooLongs` object, the `dot3StatsAlignmentErrors` object, or the `dot3StatsFCSErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

Port Interface Statistics

Use the following command to display the interface statistics for the selected port:

show interface port {*<port number, or range of ports>***} interface-counters**

Command mode: All

```
Interface statistics for port 1
                    ifHCIn Counters            ifHCOut Counters
 Octets:                          0                   929591360
 UcastPkts:                       0                     1169045
 BroadcastPkts:                   0                     3934187
 MulticastPkts:                   0                     2425859
 Discards:                        0                         855
 Errors:                          0                           0
```

Table 3-7 Interface Statistics for Port

Statistics	Description
`ifHCIn Counters Octets`	The total number of octets received on the interface, including framing characters.
`ifHCIn Counters UcastPkts`	The number of packets, delivered by this sub-layer to a higher sub- layer, which were not addressed to a multicast or broadcast address at this sub-layer.
`ifHCIn Counters BroadcastPkts`	The number of packets, delivered by this sub-layer to a higher sub- layer, which were addressed to a broadcast address at this sub-layer.
`ifHCIn Counters MulticastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. **Note**: If you see errors indicted by this counter, check the port's ethernet-counters to determine the cause of the errors.
`ifHCIn Counters Discards`	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
`ifHCIn Counters Errors`	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
`ifHCOut Counters Octets`	The total number of octets transmitted out of the interface, including framing characters.
`ifHCOut Counters UcastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
`ifHCOut Counters BroadcastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of `ifOutBroadcastPkts`.
`ifHCOut Counters MulticastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of `ifOutMulticastPkts`.

Table 3-7 Interface Statistics for Port

Statistics	Description
`ifHCOut Counters Discards`	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
`ifHCOut Counters Errors`	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. **Note**: If you see errors indicted by this counter, check the port's ethernet-counters to determine the cause of the errors.

Port IP Statistics

Use the following command to display the interface protocol (IP) statistics for the selected port:

`show interface port {`*<port number>***`} ip-counters`**

Command mode: All

```
GEA IP statistics for port 1:
ipInReceives           : 9710
ipInHeaderError        : 0
ipInDiscards           : 0
```

Table 3-8 Port IP Statistics

Statistics	**Description**
`ipInReceives`	The total number of input datagrams received from interfaces, including those received in error.
`ipInHdrError`	The number of input datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
`ipInDiscards`	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

LACP Statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics for the selected port:

show interface port {<*port number*>**} lacp counters**

Command mode: All

```
port 1
-----------------------------------------
Valid LACPDUs received:          - 0
Valid Marker PDus received:      - 0
Valid Marker Rsp PDus received:  - 0
Unknown version/TLV type:        - 0
Illegal subtype received:        - 0
LACPDUs transmitted:             - 0
Marker PDUs transmitted:         - 0
Marker Rsp PDUs transmitted:     - 0
```

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

Table 3-9 LACP Statistics

Statistic	Description
Valid LACPDUs received	Total number of valid LACP data units received.
Valid Marker PDUs received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDUs received	Total number of valid LACP marker response data units received.
Unknown version/TLV type	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
Illegal subtype received	Total number of LACP data units with an illegal subtype received.
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

Link Statistics

Use the following command to display the link statistics for the selected port:

show interface port {*<port number, or range of ports>***} link-counters**

Command mode: All

```
Link statistics for port:1
linkStateChange:1
```

Table 3-10 Link Statistics

Statistics	Description
linkStateChange	The total number of link state changes.

Layer 2 Statistics

This section describes general Layer 2 statistics commands.

Table 3-11 Layer 2 Statistics Commands

Command Syntax and Usage
`show mac-address-table counters` Displays Forwarding Database (FDB) statistics. To view an example of the command output, see page 85. **Command mode:** All
`clear mac-address-table counters` Clears FDB statistics. **Command mode:** All except User EXEC

Forwarding Database Statistics

Use the following command to display statistics regarding the use of the Forwarding Database (FDB), including the number of new entries, finds, and unsuccessful searches:

`show mac-address-table counters`

Command mode: All

```
FDB statistics:
 current:                  85      hiwat:                 129
```

FDB statistics are described in the following table:

Table 3-12 Forwarding Database Statistics

Statistic	Description
`current`	Current number of entries in the Forwarding Database.
`hiwat`	Highest number of entries recorded at any given time in the Forwarding Database.

Layer 3 Statistics

The following table describes the commands that you can enter to view Layer 3 statistics:

Table 3-13 Layer 3 Statistics Commands

Command Syntax and Usage
`clear ip` Clears all IP statistics. **Command mode:** All except User EXEC
`clear ip arp-cache` Clears IP arp cache. **Command mode:** All except User EXEC
`show ip igmp groups` Displays source address, port number, version, Vlan and other information. **Command mode:** All
`show ip igmp counters` Displays IGMP statistics. To view an example of the command output, see page 88. **Command mode:** All
`clear ip igmp [`*<VLAN number>***`]counters`** Clears IGMP Snooping statistics counters. Enter the VLAN number to clear statistics on the selected VLAN. **Command mode:** All except User EXEC
`show layer3 counters` Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. **Command mode:** All

ARP Statistics

The following command displays Address Resolution Protocol (ARP) statistics:

show ip arp counters

Command mode: All

```
ARP Statistics:
arpEntriesCur:    2      arpEntriesHighWater:     4
arpEntriesMax:    4000
```

Table 3-14 ARP Statistics

Statistics	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.

IGMP Statistics

The following command displays statistics about the use of the IGMP Multicast Groups:

`show ip igmp counters`

Command mode: All

```
IGMP Snoop vlan 1 statistics
------------------------------
rxIgmpValidPkts:                  0
rxIgmpInvalidPkts:                0
rxIgmpGenQueries:                 0
rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:    0
rxIgmpLeaves:                     0
rxIgmpReports:                    0
txIgmpReports:                    0
txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                     0
rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:  0
rxIgmpV3FilterChangeRecords:      0
```

Table 3-15 IGMP Statistics

Statistic	Description
`rxIgmpValidPkts`	Total number of valid IGMP packets received.
`rxIgmpInvalidPkts`	Total number of invalid packets received.
`rxIgmpGenQueries`	Total number of General Membership Query packets received.
`rxIgmpGrpSpecificQueries`	Total number of Group Specific Queries received.
`rxIgmpGroupSrcSpecificQueries`	Total number of Group Source-Specific Queries (GSSQ) received.
`rxIgmpLeaves`	Total number of Leave requests received.
`rxIgmpReports`	Total number of Membership Reports received.
`txIgmpReports`	Total number of Membership reports transmitted.
`txIgmpGrpSpecificQueries`	Total number of Membership Query packets transmitted to specific groups.
`txIgmpLeaves`	Total number of Leave messages transmitted.
`rxIgmpV3CurrentStateRecords`	Total number of Current State records received.

Table 3-15 IGMP Statistics

Statistic	Description
`rxIgmpV3SourceListChangeRecords`	Total number of Source List Change records received.
`rxIgmpV3FilterChangeRecords`	Total number of Filter Change records received.

Access Control List Statistics

Table 3-16 ACL Statistics Commands

Command Syntax and Usage Need information on all following statistics

`show access-control list {<1-768>} counters`

Displays the Access Control List Statistics for a specific ACL.

Command mode: All

For details, see page 90.

`show access-control counters`

Displays all ACL statistics.

Command mode: All except User EXEC

`clear access-control list`

Clears ACL statistics.

Command mode: All except User EXEC

ACL Statistics

This option displays ACL statistics.

`show access-control counters`

Command mode: All

```
Hits for ACL 1, port EXT1:              26057515
Hits for ACL 2, port EXT1:              26057497
```

Management Processor Statistics

The following table describes the commands used to display statistics about the switch's management processor.

Table 3-17 Management Processor Statistics commands

Command Syntax and Usage
`show mp memory` Displays system memory statistics. **Command mode:** All
`show mp packet` Displays packet statistics, to check for leads and load. **Command mode:** All
`show mp tcp-block` Displays all Transmission Control Protocol (TCP) control blocks (TCB) that are in use. **Command mode:** All To view a sample output, see page 91.
`show mp udp-block` Displays all User Datagram Protocol (UDP) control blocks (UCB) that are in use. **Command mode:** All To view a sample output, see page 92.
`show mp cpu` Displays CPU utilization for periods of up to 1, 5, and 15 minutes. **Command mode:** All To view a sample output, see page 93.

TCP Statistics

The following command displays TCP statistics:

show mp tcp-block

Command mode: All

```
TCP ALLOCATED CONTROL BLOCKS
12.16.20.10    443 <=>   10.10.10.112  3804        LISTEN
12.31.80.206    23 <=>   10.10.10.127  2531   ESTABLISHED
```

Table 3-18 describes the Transmission Control Protocol (TCP) control block (TCB) statistics shown in this example:

Table 3-18 TCP Statistics

Description	Example
Destination IP address	12.16.20.10
Destination port	443
Source IP address	10.10.10.112
Source port	3804
State	Listen

UDP Statistics

The following command displays UDP statistics:

`show mp udp-block`

Command mode: All

```
UDP ALLOCATED CONTROL BLOCKS
10.10.10.12      68    LISTEN
0.0.0.0         123    LISTEN
0.0.0.0         161    LISTEN
0.0.0.0        1812    LISTEN
0.0.0.0        1813    LISTEN
0.0.0.0        6123    LISTEN
0.0.0.0        7000    LISTEN
0.0.0.0        9000    LISTEN
```

Table 3-19 describes the User Datagram Protocol (UDP) control block statistics shown in this example:

Table 3-19 UDP Statistics

Description	Example
`IP address`	10.10.10.12
`Control block`	68
`State`	Listen

CPU Statistics

The following command displays the CPU utilization statistics:

`show mp cpu`

Command mode: All except User EXEC.

```
CPU information:
Load Average (over the last 1 min):     0.45
Load Average (over the last 5 mins):    0.34
Load Average (over the last 15 mins):   0.28
Runnable tasks/Total processes:         1/57
PID of the most recent process:         274
-----------------------------------------------------------
Memory information:
        total:    used:    free:   shared:  buffers:  cached:
Mem:  203755520 143568896 60186624 34054144 62914560 24567808
...
```

CPU utilization statistics to note are listed below:

- The percentage of MP CPU utilization over 1 minute, 5 minutes, and 15 minutes.
- Total memory available
- Total memory used

SNMP Statistics

The following command displays current SNMP parameters:

`show snmp-server`

Command mode: All

```
Current SNMP params
 sysName:                  "RS G8000"
 sysLocation:              "g8000"
 sysContact:               "Blade Network Technologies"
 Read community string:    "public"
 Write community string:   "private"
 Trap source address:      12.31.80.206
 Authentication traps      disabled.
 All link up/down traps    enabled.

Current v1/v2 access enabled
```

The following command displays SNMP statistics:

`show snmp-server counters`

Command mode: All

```
SNMP statistics:
-----------------------------------------------------------------
snmpInPkts:              1351    snmpInBadVersions:             0
snmpInBadC'tyNames:      12      snmpInBadC'tyUses:             679
snmpInASNParseErrs:      660     snmpEnableAuthTraps:           2
snmpOutPkts:             1339    snmpInBadTypes:                0
snmpInTooBigs:           0       snmpInNoSuchNames              0
snmpInBadValues          0       snmpInReadOnlys                0
snmpInGenErrs            0       snmpInTotalReqVars             3343
snmpInTotalSetVars       0       snmpInGetRequests              679
snmpInGetNexts           660     snmpInSetRequests              0
snmpInGetResponses       0       snmpInTraps                    10
snmpOutTooBigs           0       snmpOutNoSuchNames             0
snmpOutBadValues         0       snmpOutReadOnlys               0
snmpOutGenErrs           0       snmpOutGetRequests             0
snmpOutGetNexts          0       snmpOutSetRequests             0
snmpOutGetResponses      0       snmpOutTraps                   0
snmpSilentDrops          12      snmpProxyDrops                 0
```

Table 3-20 SNMP Statistics

Statistics	Description
`snmpInPkts`	The total number of Messages delivered to the SNMP entity from the transport service.
`snmpInBadVersions`	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
`snmpInBadC'tyNames`	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
`snmpInBadC'tyUses`	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.
`snmpInASNParseErrs`	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
`snmpEnableAuth Traps`	An object to enable or disable the authentication traps generated by this entity (the switch).
`snmpOutPkts`	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
`snmpInBadTypes`	The total number of SNMP Messages which failed ASN parsing.
`snmpInTooBigs`	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is *too big.*
`snmpInNoSuchNames`	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
`snmpInBadValues`	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue.`

Table 3-20 SNMP Statistics

Statistics	Description
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value `read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is noSuchName.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpOutReadOnlys	Not in use.

Table 3-20 SNMP Statistics

Statistics	Description
`snmpOutGenErrs`	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr`.
`snmpOutGetRequests`	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutGetNexts`	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutSetRequests`	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutGet Responses`	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutTraps`	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpSilentDrops`	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
`snmpProxyDrops`	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned.

Statistics Dump

The following command dumps switch statistics:

`show counters`

Use the dump command to dump all switch statistics (40K or more, depending on your configuration). This data can be used to tune or debug switch performance. If you want to capture dump data to a file, set the communication software on your workstation to capture session data before issuing the dump command.

Statistics Dump Output Example

The following command show a partial example of the output of the show counters command.

`show counters`

Command mode: All

```
------------------------------------------------------
Interface statistics for port 1
                   ifHCIn Counters     ifHCOut Counters
 Octets:                         0                    0
 UcastPkts:                      0                    0
 BroadcastPkts:                  0                    0
 MulticastPkts:                  0                    0
 Discards:                       0                    0
 Errors:                         0                    0

-----------------------------------------------------------
Ethernet statistics for port 1
 dot3StatsAlignmentErrors:                             0
 dot3StatsFCSErrors:                                   0
 dot3StatsSingleCollisionFrames:                       0
 dot3StatsMultipleCollisionFrames:                     0
 dot3StatsLateCollisions:                              0
 dot3StatsExcessiveCollisions:                         0
 dot3StatsInternalMacTransmitErrors:                   0
 dot3StatsFrameTooLongs:                               0
 dot3StatsInternalMacReceiveErrors:                    0
------------------------------------------------------------------
...
```

CHAPTER 4

Configuration Commands

This chapter explains how to use the Command Line Interface (CLI) to make, view and save switch configuration changes.

Table 4-1 General Configuration Commands

Command Syntax and Usage
`copy running-config startup-config` Copy the current (running) configuration from switch memory to the startup-config partition in flash (save the new configuration). **Command mode:** All except User EXEC
`copy running-config {ftp|tftp}` Backs up current configuration to a file on the selected FTP/TFTP server. **Command mode:** All except User EXEC
`copy running-config backup-config` Copy the current (running) configuration from switch memory to the backup-config partition. **Command mode:** All except User EXEC
`copy active-config running-config` Copy the active (saved) configuration from switch memory to the running-config partition. **Command mode:** All except User EXEC
`copy active-config {ftp|tftp}` Copy the active (saved) configuration from switch memory to a file on the selected FTP/TFTP server. **Command mode:** All except User EXEC
`copy backup-config running-config` Copy the backup configuration from switch memory to the running-config partition. **Command mode:** All except User EXEC

Table 4-1 General Configuration Commands

Command Syntax and Usage
`copy backup-config {ftp|tftp}` Copy the backup configuration from switch memory to a file on the selected FTP/TFTP server. **Command mode:** All except User EXEC
`show running-config` Dumps the current configuration to a script file. **Command mode:** All
`show active-config` Dumps the active switch configuration to the terminal screen. **Command mode:** All
`show backup-config` Dumps the backup switch configuration to the terminal screen. **Command mode:** All
`show startup-config` Dumps the startup switch configuration to the terminal screen. **Command mode:** All

Viewing and Saving Changes

As you use the configuration commands to set switch parameters, the changes you make take effect immediately. You do not need to apply them. Configuration changes are lost the next time the switch boots, unless you save the changes.

Note – Some operations can override the settings of the Configuration commands. The Information commands display current run-time information of switch parameters.

Saving the Configuration

You must save configuration settings to Flash memory, so the switch reloads the settings after a reset.

Note – If you do not save the changes, they will be lost the next time the system is reset/rebooted.

To save the new configuration, enter the following command:

```
RS G8000# copy running-config startup-config
```

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reset, see "Selecting a Configuration Block" on page 180.

System Configuration

Use these commands to configure switch management parameters.

Table 4-2 System Configuration Commands

Command Syntax and Usage
`system date` *<yyyy> <mm> <dd>* Sets the system date. **Command mode:** Global configuration
`system time` *<hh>*`:`*<mm>*`:`*<ss>* Configures the system time using a 24-hour clock format. **Command mode:** Global configuration
`system idle` *<1-60>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is five minutes. **Command mode:** Global configuration
`[no] system timezone` Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc. **Command mode:** Global configuration
`show system timezone` Displays the current time zone configuration. **Command mode:** All except User EXEC
`[no] system daylight` Disables or enables Daylight Savings Time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. The default value is `disabled`. **Command mode:** Global configuration
`show system daylight` Displays the current Daylight Savings Time configuration. **Command mode:** All except User EXEC
`[no] system olddaylight` Enables or disables use of the Daylight Saving Time (DST) rules in effect prior to the year 2007. The default setting is `disabled`. **Command mode:** Global configuration

Table 4-2 System Configuration Commands

Command Syntax and Usage
`[no] system notice` *<1-255 characters>* Configures the contents of the first notice that you want users to see before they login to the console CLI. This notice can contain up to 255 characters and new lines. All notices are displayed when you enter the following command: **`show system`** **Command mode:** Global configuration
`[no] banner` *<1-255 characters>* Configures a login banner of up to 255 characters. After a user or administrator logs into the switch, the login banner is displayed. **Command mode:** Global configuration
`terminal-length` *<0-300>* Configures the number of lines per screen on the terminal console. **Command mode:** All except User EXEC
`hostname` *<1-64 characters>* Enables displaying of the host name (system administrator's name) in the CLI. **Command mode:** Global configuration
`[no] system dhcp` Enables or disables Dynamic Host Control Protocol for setting the IP address on the management interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default value is `enabled`. **Command mode:** Global configuration
`[no] system reset-control` Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. **Command mode:** Global configuration
`show system` Displays the current system parameters. **Command mode:** All

System Host Log Configuration

Table 4-3 Host Log Configuration Commands

Command Syntax and Usage
logging host {*<1-2>***} address {***<IP address>***}** Sets the IP address of the selected syslog host. **Command mode:** Global configuration
logging host {*<1-2>***} facility {***<0-7>***}** Sets the facility level of the selected syslog host displayed. The default is zero. **Command mode:** Global configuration
logging host {*<1-2>***} severity {***<0-7>***}** Sets the severity level of the selected syslog host displayed. The default is seven, which means log all severity levels. **Command mode:** Global configuration
no logging host {*<1-2>***}** Deletes the selected host instance. **Command mode:** Global configuration
[no] logging console Enables or disables delivery of syslog messages to the console and Telnet/SSH sessions. The default value is `enabled`. **Command mode:** Global configuration
[no] logging log [*<feature>***]** Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as VLAN or UFD), or enable/disable syslog on all available features. **Command mode:** Global configuration
show logging messages Displays the current system log (syslog) messages. **Command mode:** All
show logging Displays the current system log (syslog) settings. **Command mode:** All

SSH Server Configuration

These commands enable Secure Shell access from any SSH client.

Table 4-4 SSH Server Configuration Commands

Command Syntax and Usage
`ssh interval` *<0-24>* Sets the interval, in hours, for auto-generation of the RSA server key. **Command mode:** Global configuration
`ssh generate-host-key` Generates the RSA host key. **Command mode:** Global configuration
`ssh generate-server-key` Generates the RSA server key. **Command mode:** Global configuration
`ssh port` *<TCP port number>* Sets the SSH server port number. **Command mode:** Global configuration
`[no] ssh enable` Enables or disables the SSH server. **Command mode:** Global configuration
`show ssh` Displays the current SSH server configuration. **Command mode:** All

RADIUS Server Configuration

Table 4-5 RADIUS Configuration Commands

Command Syntax and Usage

`[no] radius-server primary-host` *<IP address>*

Defines the primary RADIUS server address.

Command mode: Global configuration

`[no] radius-server secondary-host` *<IP address>*

Defines the secondary RADIUS server address.

Command mode: Global configuration

`radius-server primary-host {`*<IP address>***`} key`** *<1-32 characters>*

This is the primary shared secret between the switch and the RADIUS server(s).

Command mode: Global configuration

`radius-server secondary-host {`*<IP address>***`} key`** *<1-32 characters>*

This is the secondary shared secret between the switch and the RADIUS server(s).

Command mode: Global configuration

`radius-server retransmit` *<1-3>*

Sets the number of failed authentication requests before switching to a different RADIUS server. The default value is three requests.

Command mode: Global configuration

`radius-server timeout` *<1-10>*

Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is three seconds.

Command mode: Global configuration

`[no] radius-server enable`

Enables or disables the RADIUS server.

Command mode: Global configuration

`radius-server port` *<1500-3000>*

Sets RADIUS port number.

Command mode: Global configuration

Table 4-5 RADIUS Configuration Commands

Command Syntax and Usage
`[no] radius-server backdoor` Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is `disabled`. To obtain the RADIUS backdoor password, contact your Service and Support line. **Command mode:** Global configuration
`[no] radius-server secure-backdoor` Enables or disables RADIUS secure back door access through Telnet/SSH only when the RADIUS servers cannot be reached. This feature is recommended to permit access to the switch when the RADIUS servers are not available. The default setting is `enabled`. **Command mode:** Global configuration
`show radius-server` Displays the current RADIUS server parameters. **Command mode:** All

TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. (Both TACACS and TACACS+ are described in RFC 1492.)

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

Table 4-6 TACACS+ Server Commands

Command Syntax and Usage
`[no] tacacs-server primary-host` *<IP address>* Defines the primary TACACS+ server address. **Command mode:** Global configuration
`[no] tacacs-server secondary-host` *<IP address>* Defines the secondary TACACS+ server address. **Command mode:** Global configuration
`[no] tacacs-server primary-host` *<IP address>* **`key`** *<1-32 characters>* Sets the primary-host key. This is the primary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
`[no] tacacs-server secondary-host` *<IP address>* **`key`** *<1-32 characters>* Sets the primary-host key. This is the secondary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
`tacacs-server port` *<1-65000>* Sets the number of the TCP port to be configured, between 1 and 65000. The default is 49. **Command mode:** Global configuration
`tacacs-server retransmit` *<1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default value is three requests. **Command mode:** Global configuration
`tacacs-server timeout` *<4-15>* Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default value is five seconds. **Command mode:** Global configuration
`tacacs-server user-mapping {`*<0-15>* **`user|oper|admin}`** Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level. **Command mode:** Global configuration
`[no] tacacs-server privilege-mapping` Enables or disables TACACS+ privilege mapping. **Command mode:** Global configuration

Table 4-6 TACACS+ Server Commands

Command Syntax and Usage
`[no] tacacs-server secure-backdoor` Enables or disables TACACS+ secure back door access through Telnet/SSH only when the TACACS+ servers cannot be reached. This feature is recommended to permit access to the switch when the TACACS+ servers are not available. The default setting is `enabled`. **Command mode:** Global configuration
`[no] tacacs-server command-authorization` Enables or disables TACACS+ command authorization. **Command mode:** Global configuration
`[no] tacacs-server command-logging` Enables or disables TACACS+ command logging. **Command mode:** Global configuration
`[no] tacacs-server enable` Enables or disables the TACACS+ server. The default setting is `disabled`. **Command mode:** Global configuration
`show tacacs-server` Displays current TACACS+ configuration parameters. **Command mode:** All

NTP Server Configuration

These commands enable you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 4-7 NTP Configuration Commands

Command Syntax and Usage
`[no] ntp primary-server` *<IP address>* Sets the IP address of the primary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
`[no] ntp secondary-server` *<IP address>* Sets the IP address of the secondary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
`ntp interval` *<5-44640>* Specifies how often, in minutes, to resynchronize the switch clock with the NTP server. **Command mode:** Global configuration
`[no] ntp enable` Enables or disables the NTP synchronization service. **Command mode:** Global configuration
`show ntp` Displays the current NTP service settings and NTP statistics. **Command mode:** All

System SNMP Configuration

The switch supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 4-8 System SNMP Commands

Command Syntax and Usage
`[no] snmp-server name` *<1-64 characters>* Configures the name for the system. **Command mode:** Global configuration
`[no] snmp-server location` *<1-64 characters>* Configures the name of the system location. **Command mode:** Global configuration
`[no] snmp-server contact` *<1-64 characters>* Configures the name of the system contact. **Command mode:** Global configuration
`snmp-server read-community` *<1-32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. The default read community string is *public*. **Command mode:** Global configuration
`snmp-server write-community` *<1-32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. The default write community string is *private*. **Command mode:** Global configuration

Table 4-8 System SNMP Commands

Command Syntax and Usage
`[no] snmp-server authentication-trap enable` Enables or disables the use of the system authentication trap facility. The default setting is `disabled`. **Command mode:** Global configuration
`[no] snmp-server link-trap port` *<port number>* Enables or disables the sending of SNMP link up and link down traps. The default setting is `enabled`. **Command mode:** Global configuration
`show snmp-server` Displays the current SNMP configuration. **Command mode:** All

SNMPv3 Configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- A new SNMP message format
- Security for messages
- Access control
- Remote configuration of SNMP parameters

For more details about the SNMPv3 architecture see RFC2271 to RFC2276.

Table 4-9 SNMPv3 Configuration Commands

Command Syntax and Usage
`snmp-server user` *<1-16>* Configures a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. **Command mode:** Global configuration
`snmp-server view` *<1-128>* Allows you to create different MIB views. **Command mode:** Global configuration
`snmp-server access` *<1-32>* Allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification requests from an SNMP entity. **Command mode:** Global configuration
`snmp-server group` *<1-16>* Maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view command options, see page 118. **Command mode:** Global configuration
`snmp-server community` *<1-16>* Sets the SNMP-server community parameter. The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view command options, see page 119. **Command mode:** Global configuration

Table 4-9 SNMPv3 Configuration Commands

`snmp-server target-address` *<1-16>*

Allows you to configure destination information, consisting of a transport domain and a transport address, also known as a transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view command options, see page 120.

Command mode: Global configuration

`snmp-server target-parameters` *<1-16>*

Allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view command options, see page 121.

Command mode: Global configuration

`snmp-server notify` *<1-16>*

Sets the SNMP-server notification parameter. A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Command mode: Global configuration

`snmp-server version v1v2v3`

Allows SNMPv1/SNMPv2/SNMPv3 access.

Command mode: Global configuration

`snmp-server version v3only`

Allows only SNMP version 3 access.

Command mode: Global configuration

`show snmp-server v3`

Displays the current SNMPv3 configuration.

Command mode: All

User Security Model Configuration

You can make use of a defined set of user identities using this User Security Mode (USM). An SNMP engine must have the knowledge of applicable attributes of a user. These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

Table 4-10 User Security Model Configuration Commands

Command Syntax and Usage

`snmp-server user` *<1-16>* **`name`** *<1-32 characters>*

Allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch.

Command mode: Global configuration

`no snmp-server user` *<1-16>*

Deletes the selected USM user entry.

Command mode: Global configuration

`snmp-server user {`*<1-16>***`}authentication-protocol {md5|sha|none} authentication-password`** *<password value>*

Allows you to configure the authentication protocol and password.

The authentication protocol can be HMAC-MD5-96 (`md5`) or HMAC-SHA-96 (`sha`), or `none`. The default algorithm is `none`.

After you select an authentication protocol, you must provide the authentication password, otherwise you will get an error message during validation.

Command mode: Global configuration

`snmp-server user {`*<1-16>***`} privacy-protocol {des|none} privacy-password`** *<password value>*

Allows you to configure the type of privacy protocol and the privacy password.

The privacy protocol protects messages from disclosure. The options are `des` (CBC-DES Symmetric Encryption Protocol) or `none`. If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select `none` as the authentication protocol, you will get an error message.

You can create or change the privacy password.

Command mode: Global configuration

`show snmp-server v3 user` *<1-16>*

Displays the USM user entries.

Command mode: All

SNMPv3 View Configuration

Table 4-11 SNMPv3 View Configuration Commands

Command Syntax and Usage
`snmp-server view {`*<1-128>***`} name`** *<1-32 characters>* Defines the name for a family of view subtrees. **Command mode:** Global configuration
`snmp-server view {`*<1-128>***`} tree`** *<object identifier>* Defines the Object Identifier (OID), a text string which, when combined with the corresponding mask, defines a family of view subtrees. An example of an OID is 1.3.6.1.2.1.1.1.0 **Command mode:** Global configuration
`snmp-server view {`*<1-128>***`} mask`** *<1-32 characters>* Defines the bit mask, which in combination with the corresponding tree, defines a family of view subtrees. **Command mode:** Global configuration
`snmp-server view {`*<1-128>***`} type {included|excluded}`** Selects whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view. **Command mode:** Global configuration
`show snmp-server v3 view` *<1-128>* Displays the current `vacmViewTreeFamily` configuration. **Command mode:** All

View-Based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

Table 4-12 View-based Access Control Model Commands

Command Syntax and Usage
`snmp-server access {`*<1-32>***`} name`** *<1-32 characters>* Defines the name of the group. **Command mode:** Global configuration
`snmp-server access {`*<1-32>***`} security {usm|snmpv1|snmpv2}`** Allows you to select the security model to be used. **Command mode:** Global configuration
`snmp-server access {`*<1-32>***`} level {noauthnopriv|authnopriv|authpriv}`** Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode:** Global configuration
`snmp-server access {`*<1-32>***`} read-view`** *<1-32 characters>* Defines a read view name that allows read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value, then no access is granted. **Command mode:** Global configuration
`snmp-server access {`*<1-32>***`} write-view`** *<1-32 characters>* Defines a write view name that allows write access to the MIB view. If the value is empty or if there is no active MIB view having this value, then no access is granted. **Command mode:** Global configuration
`snmp-server access {`*<1-32>***`} notify-view`** *<1-32 characters>* Defines a notify view name that allows notify access to the MIB view. **Command mode:** Global configuration
`show snmp-server v3 access {`*<1-32>***`}`** Displays the View-based Access Control configuration. **Command mode:** All

SNMPv3 Group Configuration

Table 4-13 SNMPv3 Group Configuration Commands

Command Syntax and Usage
snmp-server group {<*1-16*>**} security {usm|snmpv1|snmpv2}** Defines the security model. **Command mode:** Global configuration
snmp-server group {<*1-16*>**} user-name** <*1-32 characters*> Sets the user name as defined in the following command: `snmp-server user` <*1-16*> `name` <*1-32 characters*>. **Command mode:** Global configuration
snmp-server group {<*1-16*>**} group-name** <*1-32 characters*> Sets the name for the access group. **Command mode:** Global configuration
show snmp-server v3 group {<*1-16*>**}** Displays the current `vacmSecurityToGroup` configuration. **Command mode:** All

SNMPv3 Community Table Configuration

Use these commands to configure the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of the SNMP engine.

Table 4-14 SNMPv3 Community Table Configuration Commands

Command Syntax and Usage
`snmp-server community {`*<1-16>***`} index`** *<1-32 characters>* Allows you to configure the unique index value of a row in this table. **Command mode:** Global configuration
`snmp-server community {`*<1-16>***`} name`** *<1-32 characters>* Defines a readable text string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** Global configuration
`snmp-server community {`*<1-16>***`} user-name`** *<1-32 characters>* Defines a readable text string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** Global configuration
`snmp-server community {`*<1-16>***`} tag`** *<1-255 characters>* Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode:** Global configuration
`show snmp-server v3 community {`*<1-16>***`}`** Displays the community table configuration. **Command mode:** All

SNMPv3 Target Address Table Configuration

These commands allow you to set passwords and display current user statistics. Passwords can be a maximum of 15 characters. To disable a user, set the password to null.

Table 4-15 Target Address Table Configuration Commands

Command Syntax and Usage
`snmp-server target-address {`*<1-16>***`} address {`***<IP address>***`} name`** *<1-32 characters>* Configures the locally arbitrary, but unique identifier, target address name associated with this entry. **Command mode:** Global configuration
`snmp-server target-address {`*<1-16>***`} name {`***<1-32 characters>***`} address`** *<transport IP address>* Configures a transport address IP that can be used in the generation of SNMP traps. **Command mode:** Global configuration
`snmp-server target-address {`*<1-16>***`} taglist`** *<1-255 characters>* Configures a list of tags that are used to select target addresses for a particular operation. **Command mode:** Global configuration
`snmp-server target-address {`*<1-16>***`} parameters-name`** *<1-32 characters>* Defines the name as defined in the following command: `snmp-server target-parameters {`*<1-16>*`} name` *<1-32 characters>*. **Command mode:** Global configuration
`no snmp-server target-address {`*<1-16>***`}`** Deletes the Target Address Table entry. **Command mode:** Global configuration
`show snmp-server v3 target-address {`*<1-16>***`}`** Displays the current Target Address Table configuration. **Command mode:** All

SNMPv3 Target Parameters Table Configuration

You can configure the Target Parameters entry and store it in the Target Parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthnoPriv`, `authNoPriv`, or `authPriv`).

Table 4-16 Target Parameters Table Configuration Commands

Command Syntax and Usage
`snmp-server target-parameters {`*<1-16>***`} name`** *<1-32 characters>* Configures the locally arbitrary, but unique identifier that is associated with this entry. **Command mode:** Global configuration
`snmp-server target-parameters {`*<1-16>***`} message {snmpv1|snmpv2c|snmpv3}`** Configures the message processing model used to generate SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters {`*<1-16>***`} security {usm|snmpv1|snmpv2}`** Selects the security model to be used when generating the SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters {`*<1-16>***`} user-name`** *<1-32 characters>* Defines the name that identifies the user in the USM table on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration

`snmp-server target-parameters {`*<1-16>***`}`**
`level {noAuthNoPriv|authNoPriv|authPriv}`
Selects the level of security to be used when generating the SNMP messages using this entry. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.
Command mode: Global configuration

`show snmp-server v3 target-parameters {`*<1-16>***`}`** Displays the current `targetParamsTable` configuration. **Command mode:** All

SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Table 4-17 Notify Table Commands

Command Syntax and Usage
`snmp-server notify {`*<1-16>***`} name`** *<1-32 characters>* Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry. **Command mode:** Global configuration
`snmp-server notify {`*<1-16>***`} tag`** *<1-255 characters>* Configures a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag, is selected. **Command mode:** Global configuration
`show snmp-server v3 notify {`*<1-16>***`}`** Displays the current notify table configuration. **Command mode:** All

System Access Configuration

Table 4-18 System Access Configuration Commands

Command Syntax and Usage

`[no] access http enable`

Enables or disables HTTP (Web) access to the Browser-Based Interface.
The default value is `enabled`.

Command mode: Global configuration

`[default] access http port [`*<1-65535>***`]`**

Sets the switch port used for serving switch Web content. The default is HTTP port `80`.

Command mode: Global configuration

`[no] access userbbi enable`

Enables or disables user configuration access to the Browser-Based Interface (BBI).

Command mode: Global configuration

`[no] access telnet enable`

Enables or disables Telnet access. The default value is `enabled`.

Command mode: Global configuration

`[default] access telnet port` *<1-65535>*

Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port.

Command mode: Global configuration

`[default] access tftp-port` *<1-65535>*

Sets the TFTP server port number for file transfers.

Command mode: Global configuration

`[no] access snmp {read-only|read-write}`

Provides read-only/write-read SNMP access.

Command mode: Global configuration

`show access`

Displays the current system access parameters.

Command mode: All

HTTPS Access Configuration

Table 4-19 HTTPS Access Configuration Commands

Command Syntax and Usage

`[no] access https enable`

Enables BBI access (Web access) using HTTPS. The default value is `disabled`.

Command mode: Global configuration

`[default] access https port [`*<1-65535>*`]`

Defines the HTTPS Web server port number.

Command mode: Global configuration

`access https generate-certificate`

Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:

- Country Name (2 letter code) [ ]: CA
- State or Province Name (full name) []: Ontario
- Locality Name (for example, city) []: Ottawa
- Organization Name (for example, company) []: Blade
- Organizational Unit Name (for example, section) []: DataCenter
- Common Name (for example, user's name) []: Mr Smith
- Email (for example, email address) []: info@bladenetworks.net

You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.

Command mode: Global configuration

`access https save-certificate`

Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.

Command mode: Global configuration

`show access`

Displays the current system access configuration.

Command mode: All except User EXEC

Management Network Configuration

These commands are used to define IP address ranges which are allowed to access the switch for management purposes.

Table 4-20 Management Network Configuration Commands

Command Syntax and Usage
`access management-network` *<IP address> <IP mask>* Adds a defined network through which switch access is allowed through Telnet, SNMP, SSH, or the browser-based interface (BBI). A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Note**: If you configure the management network without including the switch interfaces, it will cause the Firewall Load Balancing health checks to fail and will create a "Network Down" state on the network. **Command mode:** Global configuration
`no access management-network` *<IP address> <IP mask>* Removes a defined network, which consists of a management network address and a management network mask address. **Command mode:** Global configuration
`show access management-network` Displays the current configuration. **Command mode:** All except User EXEC
`clear access management-network` Removes all defined management networks. **Command mode:** Global configuration

User Access Control Configuration

The following table describes user-access control commands.

NOTE – User passwords can be a maximum of 128 characters.

Table 4-21 User Access Control Configuration Commands

Command Syntax and Usage

`access user administrator-password`
`access user operator-password`
`access user user-password`
Allows you to change the password. You must enter the current password for validation.
Command Mode: Global configuration

`access user` *<1-10>* Configures the User ID. **Command mode:** Global configuration
`access user eject [console-user]` Ejects the current console user from the switch. **Command mode:** Global configuration
`access user eject` *<user name>* **[***<IP address>***] [***<Telnet/SSH port number>***]** Ejects the specified user(s) from the switch. **Command mode:** Global configuration
`access user user-password` *<1-128 characters>* Sets the user (`user`) password. The user has no direct responsibility for switch management. The user can view switch status information and statistics, but cannot make any configuration changes. **Command mode:** Global configuration

Table 4-21 User Access Control Configuration Commands

Command Syntax and Usage
`access user operator-password` *<1-128 characters>* Sets the operator (`oper`) password. The operator has no direct responsibility for switch management. The operator can view switch status information and statistics, but cannot make any configuration changes. **Command mode:** Global configuration
`access user administrator-password` *<1-128 characters>* Sets the administrator (`admin`) password. The super user administrator has complete access to all information and configuration commands on the switch, including the ability to change both the user and administrator passwords. Access includes "`oper`" functions. **Command mode:** Global configuration
`show access user` Displays the current user status. **Command mode:** All except User EXEC

System User ID Configuration

Table 4-22 User ID Configuration Commands

Command Syntax and Usage
`access user {`*<1-10>***`} level {administrator|operator|user}`** Sets the Class-of-Service to define the user's authority level. The switch defines these levels as: User, Operator, and Administrator, with User being the most restricted level. **Command mode:** Global configuration
`access user {`*<1-10>***`} name`** *<1-8 characters>* Defines the user name. **Command mode:** Global configuration
`access user {`*<1-10>***`} password`** *<1-128 characters>* Sets the user password. **Command mode:** Global configuration
`[no] access user {`*<1-10>***`} enable`** Enables or disables the user ID. **Command mode:** Global configuration
`show access user` Displays the current user ID configuration. **Command mode:** All except User EXEC

Port Configuration

Use the Interface port commands to configure settings for individual switch ports.

Table 4-23 Port Configuration Commands

Command Syntax and Usage

`interface port` *<port number>*

Enter Interface Port configuration mode for the selected port.

Command mode: Global configuration

`interface portchannel` *<trunk group number>*

Enter Interface PortChannel (trunk group) configuration mode for the selected trunk group. This mode allows you to configure port settings for the trunk group.

Command mode: Global configuration

`[no] auto`

Configures the port's transmission media as automatic.

Command mode: Interface port

`[no] bpdu-guard`

Enables or disables BPDU Guard. If Spanning Tree BPDUs are received on the port, BPDU Guard disables the port.

Command mode: Interface port

`dot1p` *<0-7>*

Configures the port's 802.1p priority level.

Command mode: Interface port

`[no] dscp-marking`

Enables or disables DSCP re-marking on a port.

Command mode: Interface port

`[no] name` *<1-64 characters>*

Configures a name for the port. The assigned port name displays next to the port number on some information and statistics screens.

Command mode: Interface port

`pvid` *<1-4094>*

Sets the default VLAN number which will be used to forward frames which are not VLAN tagged.

Command mode: Interface port

Table 4-23 Port Configuration Commands

Command Syntax and Usage
`[no] shutdown` Disables the port. To temporarily disable a port without changing its configuration attributes, see see "Temporarily Disabling a Port" on page 130. **Command mode:** Interface port
`[no] tag-pvid` Enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is `enabled`. **Command mode:** Interface port
`[no] tagging` Enables VLAN tagging for this port. The default setting is `disabled`. **Command mode:** Interface port
`show interface port` *<port number>* Displays the configured port parameters. **Command mode:** All

Port Link Configuration

Use these commands to set port parameters for the port link, such as duplex, flow control, and negotiation mode for the port link.

NOTE – The speed and mode parameters are fixed for 10 Gigabit and 1 Gigabit Ethernet fixed ports, and cannot be configured.

Table 4-24 Port Link Configuration Commands

Command Syntax and Usage
`speed {10|100|1000|auto}` Sets the link speed. Not all options are valid on all ports. The choices include: ■ 10=10 megabits ■ 100=100 megabits ■ 1000=1 gigabit ■ "Auto," for auto-negotiation **Command mode:** Interface port.

Table 4-24 Port Link Configuration Commands

Command Syntax and Usage
`duplex {full|half|any}` Sets the operating mode. Not all options are valid on all ports. Ports 1-18 are set to full duplex, and cannot be changed. The choices include: ■ Full-duplex ■ Half-duplex ■ "Any," for auto-negotiation (default) **Command mode:** Interface port
`[no] flowcontrol {both|receive|send}` Sets the flow control. The choices include: ■ Both receive and transmit flow control (default) ■ Receive (rx) flow control ■ Transmit (tx) flow control **Command mode:** Interface port
`show interface port` *<port number>* Displays current port parameters. **Command mode:** All

Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
RS G8000# interface port <port number> shutdown
```

Because this configuration sets a temporary state for the port, the port state will revert to its original configuration when the switch is reset. See the "Operations Commands" on page 173 for other operations-level commands.

Port ACL Configuration

Table 4-25 Port ACL Configuration

Command Syntax and Usage
`access-control list` *<1-768>* Adds the specified ACL to the port. You can add multiple ACL lists to a port. **Command mode:** Interface port
`no access-control list` *<1-768>* Deletes the specified ACL from the port. **Command mode:** Interface port
`access-control group` *<1-768>* Adds the specified ACL Group to the port. You can add multiple ACL Groups to a port. **Command mode:** Interface port
`no access-control group` *<1-768>* Removes the specified ACL from the port. **Command mode:** Interface port
`show interface port {`*<port number>***`} access-control`** Displays current ACL QoS parameters. **Command mode:** All

Stacking Configuration

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration menu is used to configure a stack, and to define the Master and Backup interface that represents the stack on the network.

Table 4-26 Stacking commands

Command Syntax and Usage
`[no] stack name` *<1-32 characters>* Configures a name for the stack. **Command mode:** Global configuration
`stack backup` *<csnum (1-6)>* Defines the backup switch, based on its configured switch number (csnum). **Command mode:** Global configuration
`show stack switch-number` *<1-6>* Displays current stacking parameters. **Command mode:** All except user EXEC

Stacking Switch Configuration

Table 4-27 Stacking Switch commands

Command Syntax and Usage
stack switch-number *<csnum (1-6)>* **bind** *<asnum 1-12>* Binds the selected switch to the stack, based on its assigned switch number (asnum). **Command mode:** Global configuration
stack switch-number *<csnum (1-6)>* **mac** *<MAC address>* Binds the selected switch to the stack, based on its MAC address. **Command mode:** Global configuration
no stack switch-number *<csnum 1-6>* Deletes the selected switch from the stack. **Command mode:** Global configuration
show stack attached-switches Displays the current stacking switch parameters. **Command mode:** All except user EXEC

Master Switch Interface Configuration

Table 4-28 Master Switch Interface commands

Command Syntax and Usage
`stack master-ip-interface address` *<IP address>* [*<subnet mask>*] [*<gateway IP address>*] [*<VLAN 1-4094>*] Configures the IP address for the Master Switch Interface, using dotted decimal notation. **Command mode:** Global configuration
`stack master-ip-interface netmask` *<subnet mask>* Configures the IP subnet address mask for the interface, using dotted decimal notation. **Command mode:** Global configuration
`stack master-ip-interface vlan` *<VLAN (1-4094)>* Configures the VLAN number for this interface. **Command mode:** Global configuration
`stack master-ip-interface gateway` *<IP address>* Configures the default gateway for the Master Switch Interface. **Command mode:** Global configuration
`no stack master-ip-interface` Deletes the Master Switch Interface. **Command mode:** Global configuration
`show stack master-ip-interface` Displays the current Master Switch Interface parameters. **Command mode:** All except user EXEC

Backup Switch Interface Configuration

Table 4-29 Backup Switch Interface commands

Command Syntax and Usage
`stack backup-ip-interface address` *<IP address>* [*<subnet mask>*] [*<gateway IP address>*] [*<VLAN 1-4094>*] Configures the IP address for the Backup Switch Interface, using dotted decimal notation. **Command mode:** Global configuration
`stack backup-ip-interface netmask` *<subnet mask>* Configures the IP subnet address mask for the interface, using dotted decimal notation. **Command mode:** Global configuration
`stack backup-ip-interface vlan` *<VLAN 1-4094>* Configures the VLAN number for this interface. **Command mode:** Global configuration
`stack backup-ip-interface gateway` *<IP address>* Configures the default gateway for the Backup Switch Interface. **Command mode:** Global configuration
`no stack backup-ip-interface` Deletes the Backup Switch Interface. **Command mode:** Global configuration
`show stack backup` Displays the current Backup Switch Interface parameters. **Command mode:** All except user EXEC

Port Mirroring

Port Mirroring commands are used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to the monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage. The switch supports up to four monitor ports.

Port mirroring is disabled by default. For more information about port mirroring on the switch, see “Appendix A: Troubleshooting” in the RackSwitch G8000 *Application Guide*.

Table 4-30 Port Mirroring Configuration Commands

Command Syntax and Usage
`[no] port-mirroring enable` Enables or disables port mirroring. **Command mode:** Global configuration
`port-mirroring monitor-port` *<port number>* **`mirroring-port`** *<port number>* **`{in|out|both}`** Selects the monitor port, and adds the port to be mirrored. This command also allows you to enter the direction of the traffic, as follows: ■ **In**: ingress traffic ■ **Out**: egress traffic ■ **Both**: ingress and egress traffic **Command mode:** Global configuration
`show port-mirroring` Displays current settings of the mirrored and monitoring ports. **Command mode:** All except User EXEC

Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 4-31 Layer 2 Configuration Commands

Command Syntax and Usage
`vlan` *<1-4094>* Enters VLAN configuration mode. To view command options, see page 152. **Command mode:** Global configuration
`[no] spanning-tree bpdu-guard` Globally enables or disables BPDU Guard. If Spanning Tree BPDUs are received on a port, BPDU Guard disables the port. **Command mode:** All
`show layer2 information` Displays current Layer 2 parameters. **Command mode:** All

802.1X Configuration

These commands allow you to configure the switch as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 4-32 802.1X Configuration Commands

Command Syntax and Usage
`dot1x enable` Globally enables 802.1X. **Command mode:** Global configuration
`show dot1x information` Displays current enabled/disabled state of 802.1X parameters. **Command mode:** All

802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the switch.

Table 4-33 802.1X Global Configuration Commands

Command Syntax and Usage
`dot1x apply-global` Applies global configuration. **Command mode:** Global configuration
`dot1x max-request {`*`<1-10>`***`}`** Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is `2`. **Command mode:** Global configuration
`dot1x mode {force-unauthorized|auto|force-authorized}` Sets the type of access control for all ports: ■ **`force-unauthorized`**: The port is unauthorized unconditionally. ■ **`auto`**: The port is unauthorized until it is successfully authorized by the RADIUS server. ■ **`force-authorized`**: The port is authorized unconditionally, allowing all traffic. The default value is `force-authorized`. **Command mode:** Global configuration

Table 4-33 802.1X Global Configuration Commands

Command Syntax and Usage
`dot1x quiet-time {`*<0-65535>***`}`** Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds. **Command mode:** Global configuration
`[no] dot1x re-authenticate` Sets the re-authentication status to `on`. The default value is `off`. **Command mode:**   Global configuration
`dot1x re-authentication-interval {`*<1-604800>***`}`** Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds. **Command mode:** Global configuration
`dot1x supplicant-timeout {`*<1-65535>***`}`** Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds. **Command mode:** Global configuration
`dot1x transmit-interval {`*<1-65535>***`}`** Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds. **Command mode:** Global configuration
`[no] dot1x vlan-assign` Globally sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. This feature allows the RADIUS server to specify the VLAN for the port during 802.1x authentication. **Command mode:** Global configuration
`show dot1x` Displays current global 802.1X parameters. **Command mode:** All

802.1X Guest VLAN Configuration

The 802.1X Guest VLAN menu allows you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 2 802.1X Guest VLAN Configuration Commands

Command Syntax and Usage
[`no`] **`dot1x guest-vlan vlan`** *<VLAN number>* Configures the Guest VLAN number. **Command mode:** Global configuration
`dot1x guest-vlan enable` Enables the 802.1X Guest VLAN. **Command mode:** Global configuration
`no dot1x guest-vlan enable` Disables the 802.1X Guest VLAN. **Command mode:** Global configuration
`show dot1x` Displays current 802.1X parameters. **Command mode:** All

802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the switch. These settings override the global 802.1X parameters.

Table 4-34 802.1X Port Commands

Command Syntax and Usage
`dot1x apply-global` Applies current global 802.1X configuration parameters to the port. **Command mode:** Interface port
`dot1x mode force-unauthorized|auto|force-authorized` Sets the type of access control for the port: ■ **`force-unauthorized`** - the port is unauthorized unconditionally. ■ **`auto`** - the port is unauthorized until it is successfully authorized by the RADIUS server. ■ **`force-authorized`** - the port is authorized unconditionally, allowing all traffic. The default value is `force-authorized`. **Command mode:** Interface port
`dot1x quiet-time {`*<0-65535>***`}`** Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds. **Command mode:** Interface port
`dot1x transmit-interval {`*<1-65535>***`}`** Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds. **Command mode:** Interface port
`dot1x supplicant-timeout {`*<1-65535>***`}`** Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds. **Command mode:** Interface port
`dot1x server-timeout {`*<1-65535>***`}`** Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the following command: `radius-server timeout` **Command mode:** Interface port

Table 4-34 802.1X Port Commands

Command Syntax and Usage
`dot1x max-request {`*<1-10>***`}`** Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is two. **Command mode:** Interface port
`dot1x re-authentication-interval {`*<1-604800>***`}`** Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds. **Command mode:** Interface port
`[no] dot1x re-authenticate` Sets the re-authentication status to `on`. The default value is `off`. **Command mode:** Interface port
`[no] dot1x vlan-assign` Sets the dynamic VLAN assignment for the selected port to `on` or `off`. The default value is `off`. This feature allows the RADIUS server to specify the VLAN for the port during 802.1x authentication. **Command mode:** Interface port
`show interface port {`*<port number>***`} dot1x`** Displays current 802.1X port parameters. **Command mode:** All

FDB Configuration

Use the following commands to configure the Forwarding Database (FDB).

Table 4-35 FDB Configuration Commands

Command Syntax and Usage
`mac-address-table aging` *<10-65535>* Configures the aging value for FDB entries, in seconds. The default value is 300. **Command mode**: Global configuration
`show mac-address-table` Displays current FDB configuration. **Command mode**: All

Trunk Configuration

Trunk groups (portchannels) can provide super-bandwidth connections between switches or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. The following restrictions apply to trunk group configuration:

- Any physical switch port can belong to no more than one trunk group.
- Up to eight ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same link configuration (speed, duplex, flow control).
- Trunking from non-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 4-36 Trunk Configuration Commands

Command Syntax and Usage
portchannel {<*trunk number*>**} port {**<*port number*>**}** Adds a physical port to the selected trunk group. **Command mode:** Global configuration
no portchannel {<*trunk number*>**} port {**<*port number*>**}** Removes a physical port from the selected trunk group. **Command mode:** Global configuration
[no] portchannel {<*trunk number*>**} enable** Enables or disables the current trunk group. The default value is `enabled`. **Command mode:** Global configuration
show portchannel {<*trunk number*>**}** Displays current static trunk group parameters. **Command mode:** All
show portchannel {<*LACP trunk number*>**}** Displays current LACP trunk group parameters. **Command mode:** All

IP Trunk Hash Configuration

Trunk hash parameters are set globally for the switch. You can enable one or two parameters to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

Use the following commands to configure Layer 2 IP trunk hash parameters. The trunk hash settings affect both static trunks and LACP trunks.

Table 4-37 Layer 2 IP Trunk Hash Commands

Command Syntax and Usage
`portchannel hash source-ip-address` Enables trunk hashing on the source IP address. **Command mode:** Global configuration
`portchannel hash destination-ip-address` Enables trunk hashing on the destination IP address. **Command mode:** Global configuration
`portchannel hash source-destination-ip` Enables trunk hashing on the source and destination IP address. **Command mode:** Global configuration
`portchannel hash source-mac-address` Enables trunk hashing on the source MAC address. **Command mode:** Global configuration

Table 4-37 Layer 2 IP Trunk Hash Commands

Command Syntax and Usage
`portchannel hash destination-mac-address` Enables trunk hashing on the destination MAC address. **Command mode:** Global configuration
`portchannel hash source-destination-mac` Enables trunk hashing on the source and destination MAC address. **Command mode:** Global configuration
`show portchannel hash` Displays current Layer 2 trunk hash setting. **Command mode:** All

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP).

Table 4-38 Link Aggregation Control Protocol Commands

Command Syntax and Usage
`lacp system-priority {`*<1-65535>***`}`** Defines the priority value for the switch. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Global configuration
`lacp timeout {short|long}` Defines the timeout period before invalidating LACP data from a remote partner. Choose **`short`** (3 seconds) or **`long`** (90 seconds). The default value is **`long`**. **Note**: It is recommended that you use a timeout value of **`long`**, to reduce LACPDU processing. If the CPU utilization rate of your switch remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP. **Command mode:** Global configuration

Table 4-38 Link Aggregation Control Protocol Commands

<table>
<tr><th>Command Syntax and Usage</th></tr>
<tr><td><code>default lacp [system-priority|timeout]</code>
Resets LACP parameters to their default values.
<b>Command mode:</b> Global configuration</td></tr>
<tr><td><code>no lacp</code> <i>&lt;admin key&gt;</i>
Removes all port LACP configuration with the specified admin key.
<b>Command mode:</b> Global configuration</td></tr>
<tr><td><code>show lacp</code>
Displays current LACP configuration.
<b>Command mode:</b> All</td></tr>
</table>

LACP Port Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 4-39 Link Aggregation Control Protocol Port Configuration Commands

Command Syntax and Usage
`lacp mode {off|active|passive}` Sets the LACP mode for this port, as follows: ■ **`off:`** Turns LACP off for this port. You can use this port to manually configure a static trunk. The default value is **`off`**. ■ **`active:`** Turns LACP on and sets this port to active. Active ports initiate LACPDUs. ■ **`passive:`** Turns LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. **Command mode:** Interface port
`lacp priority {`*<1-65535>***`}`** Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Interface port
`lacp key {`*<1-65535>***`}`** Sets the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group. **Command mode:** Interface port
`default lacp [key|mode|priority]` Resets LACP port parameters to their default values. **Command mode:** Interface port
`show interface port {`*<port number>***`} lacp`** Displays the current LACP configuration for this port. **Command mode:** All

Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *BLADE OS Application Guide*.

Table 4-40 Layer 2 Failover Configuration Commands

Command Syntax and Usage
`failover enable` Globally turns Layer 2 Failover `on`. **Command mode:** Global configuration
`no failover enable` Globally turns Layer 2 Failover `off`. **Command mode:** Global configuration
`show failover` Displays current Layer 2 Failover parameters. **Command mode:** All

Failover Trigger Configuration

Table 4-41 Failover Trigger Configuration Commands

Command Syntax and Usage
[`no`] **`failover trigger`** *<1-8>* **`enable`** Enables or disables the Failover trigger. **Command mode:** Global configuration
`no failover trigger` *<1-8>* Deletes the Failover trigger. **Command mode:** Global configuration
`failover trigger` *<1-8>* **`limit`** *<0-1024>* Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. **Command mode:** Global configuration
`show failover trigger` *<1-8>* Displays the current failover trigger settings. **Command mode:** All except User EXEC

Failover Manual Monitor - Monitor Configuration

Use this menu to define the port link(s) to monitor. The Manual Monitor - Monitor configuration accepts only external uplink ports.

Table 4-42 Failover Manual Monitor - Monitor commands

Command Syntax and Usage
`failover trigger` *<1-8>* **`mmon monitor member`** *<port number>* Adds the selected port to the Manual Monitor - Monitor. **Command mode:** Global configuration
`no failover trigger` *<1-8>* **`mmon monitor member`** *<port number>* Removes the selected port from the Manual Monitor - Monitor. **Command mode:** Global configuration
`failover trigger` *<1-8>* **`mmon monitor portchannel`** *<trunk number>* Adds the selected trunk group to the Manual Monitor - Monitor. **Command mode:** Global configuration
`no failover trigger` *<1-8>* **`mmon monitor portchannel`** *<trunk number>* Removes the selected trunk group to the Manual Monitor - Monitor. **Command mode:** Global configuration
`failover trigger` *<1-8>* **`mmon monitor adminkey`** *<1-65535>* Adds an LACP admin key to the Manual Monitor - Monitor. LACP trunks formed with this admin key will be included in the Manual Monitor - Monitor. **Command mode:** Global configuration
`no failover trigger` *<1-8>* **`mmon monitor adminkey`** *<1-65535>* Removes an LACP admin key from the Manual Monitor - Monitor. **Command mode:** Global configuration
`show failover` Displays the current Failover settings. **Command mode:** All except User EXEC

Failover Manual Monitor - Control Configuration

Use this menu to define the port link(s) to control.

The Manual Monitor - Control configuration accepts internal and external ports, but not management ports.

Figure 4-1 Failover Manual Monitor - Control commands

Command Syntax and Usage

`failover trigger` *<1-8>* **`mmon control member`** *<port number>*

Adds the selected port to the Manual Monitor - Control.

Command mode: Global configuration

`no failover trigger` *<1-8>* **`mmon control member`** *<port number>*

Removes the selected port from the Manual Monitor - Control.

Command mode: Global configuration

`failover trigger` *<1-8>* **`mmon control portchannel`** *<trunk number>*

Adds the selected trunk group to the Manual Monitor - Control.

Command mode: Global configuration

`no failover trigger` *<1-8>* **`mmon control portchannel`** *<trunk number>*

Removes the selected trunk group to the Manual Monitor - Control.

Command mode: Global configuration

`failover trigger` *<1-8>* **`mmon control adminkey`** *<1-65535>*

Adds an LACP admin key to the Manual Monitor - Monitor. LACP trunks formed with this admin key will be included in the Manual Monitor - Control.

Command mode: Global configuration

`no failover trigger` *<1-8>* **`mmon control adminkey`** *<1-65535>*

Removes an LACP admin key from the Manual Monitor - Control.

Command mode: Global configuration

`show failover`

Displays the current Failover settings.

Command mode: All except User EXEC

VLAN Configuration

The commands in this section configure VLAN attributes, change the status of the VLAN, delete the VLAN, and change the port membership of the VLAN. By default, all VLANs are disabled except VLAN 1, which is always enabled. The switch supports a maximum of 1,024 VLANs.

Table 4-43 VLAN Configuration Commands

Command Syntax and Usage
`vlan {`*`<1-4094>`***`}`** Enters VLAN configuration mode. **Command mode:** Global configuration
`name {`*`<1-32 characters>`***`}`** Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. **Command mode:** VLAN
`[no] member {`*`<port number or port-range>`***`}`** Adds or removes port(s) delimited by ',' or an interval of ports delimited by '-'. **Command mode:** VLAN
`[no] member portchannel {`*`<trunk number>`***`}`** Adds the selected trunk group to the VLAN. **Command mode:** VLAN
`[no] member portchannel lacp {`*`<admin key>`***`}`** Adds the selected LACP admin key to the VLAN. Trunk groups that form using the selected admin key will be members of this VLAN. **Command mode:** VLAN
`[no] enable` Enables or disables the VLAN. The default value is `disabled`. **Command mode:** VLAN
`show vlan information` Displays the current VLAN configuration. **Command mode:** All

NOTE – All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging enabled.

Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

Table 4-44 Layer 3 Configuration Commands

Command Syntax and Usage
`show layer3 information` Displays the current IP configuration. **Command mode:** All

ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

Table 4-45 ARP Configuration Commands

Command Syntax and Usage
`ip arp rearp {`*<2-120>***`}`** Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes. **Command mode:** Global configuration
`show ip arp` Displays the current ARP configurations. **Command mode:** All except User EXEC

IGMP Snooping Configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards the multicast traffic only to ports connected to those servers.

Table 4-46 describes the commands used to configure IGMP Snooping.

Table 4-46 IGMP Snooping Configuration Commands

Command Syntax and Usage
`[no] ip igmp snoop enable` Enables or disables IGMP Snooping. **Command mode:** Global configuration
`ip igmp snoop timeout` *<130-1225>* Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The default value is 260. **Command mode:** Global configuration
`ip igmp snoop mrouter-timeout` *<1-600>* Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The default value is 255 seconds. **Command mode:** Global configuration
`ip igmp snoop query-interval` *<1-600>* Sets the IGMP router query interval, in seconds. The default value is 125. **Command mode:** Global configuration
`ip igmp snoop robust` *<2-10>* Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2. **Command mode:** Global configuration
`[no] ip igmp snoop flood` Configures the switch to flood unregistered IP multicast reports to all ports. The default setting is `enabled`. Command mode: Global configuration

Table 4-46 IGMP Snooping Configuration Commands

Command Syntax and Usage

`[no] ip snoop igmp cpu`

Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:

- If no Mrouter is present, drop subsequent packets with same IPMC.
- If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN.

The default setting is `enabled`.

Note: If both **`flood`** and **`cpu`** are disabled, then the switch drops all unregistered IPMC traffic.

Command mode: Global configuration

`[no] ip snoop igmp aggregate`

Enables or disables IGMP Membership Report aggregation.

Command mode: Global configuration

`ip igmp snoop source-ip` *<VLAN number (1-4094)> <IP address>*

Configures the source IP address used as a proxy for IGMP Group Specific Queries.

Command mode: Global configuration

`[no] ip igmp snoop vlan` *<1-4094>*

Adds or removes the selected VLAN(s) to IGMP Snooping.

Command mode: Global configuration

[no] **`ip igmp snoop vlan`** *<VLAN number>* **`fast-leave`**

Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.

Command mode: Global configuration

`default ip igmp snoop`

Resets IGMP Snooping parameters to their default values.

Command mode: Global configuration

`show ip igmp snoop`

Displays the current IGMP snooping parameters.

Command mode: All

IGMP Static Multicast Router Configuration

Table 4-47 describes the commands used to configure a static multicast router.

Table 4-47 IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
ip igmp mrouter {*<port number>***|***<trunk group number>***} {***<VLAN number (1-4094)>***}** *<version (1-3)>* Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2, or 3) of the multicast router. **Note**: To add a trunk group (portchannel), enter the trunk group number as follows: *po1-po104* **Command mode:** Global configuration
no ip igmp mrouter {*<port number>***|***<trunk group number>***} {***<VLAN number (1-4094)>***}** *<version (1-3)>* Removes a static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
clear ip igmp mrouter Clears all dynamic multicast routers learned the switch. **Command mode:** Global configuration
show ip igmp mrouter Displays the current IGMP Static Multicast Router parameters. **Command mode:** All except User EXEC

Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the ping, traceroute, and TFTP commands.

Table 4-48 DNS Configuration Commands

Command Syntax and Usage
`[no] ip dns domain-name` *<character string>* Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** Global configuration
`[no] ip dns primary-server` *<IP address>* Sets the IP address for the primary DNS server, using dotted decimal notation. **Command mode:** Global configuration
`[no] ip dns secondary-server` *<IP address>* Sets the IP address for the secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the secondary server will be used instead. Enter the IP address using dotted decimal notation. **Command mode:** Global configuration
`show ip dns` Displays the current Domain Name System settings. **Command mode:** Global configuration

Quality of Service Configuration

Quality of Service (QoS) commands configure the 802.1p priority value and DiffServ Code Point value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

802.1p Configuration

This feature gives the switch the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority are given forwarding preference over packets with numerically lower priority value.

Table 4-49 802.1p Configuration Commands

Command Syntax and Usage
`qos transmit-queue mapping {`*<priority (0-7)>***`} {`***<COSq number>***`}`** Maps the 802.1p priority value to a Class of Service queue (COSq) number. Enter the 802.1p priority value, followed by the Class of Service queue that handles the matching traffic. Note that priority value 7 is reserved for Stacking. **Command mode:** Global configuration
`qos transmit-queue weight-cos {`*<COSq number>***`} {`***<weight (0-15)>***`}`** Configures the weight of the selected Class of Service queue (COSq). Enter the queue number followed by the scheduling weight (0-15). **Command mode:** Global configuration
`qos transmit-queue number-cos {1|7}` Sets the number of Class of Service queues (COSq) for switch ports. Note that one COSq is reserved for Stacking. **Command mode:** Global configuration
`show qos transmit-queue` Displays the current 802.1p parameters. **Command mode:** All except User EXEC

DSCP Configuration

These commands map the DiffServ Code Point (DSCP) value of incoming packets to an 802.1p priority value.

Table 4-50 DSCP Configuration Commands

Command Syntax and Usage
`qos dscp dot1p-mapping {`*<DSCP value 0-63>***`} {`***<priority (0-7)>***`}`** Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value. **Command mode:** Global configuration
`[no] qos dscp enable` Globally turns DSCP mapping `on` or `off`. **Command mode:** Global configuration
`show qos dscp` Displays the current DSCP parameters. **Command mode:** All except User EXEC

Access Control Configuration

Use these commands to create Access Control Lists and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

Table 4-51 General ACL Configuration Commands

Command Syntax and Usage
`[no] access-control list` *<1-768>* Configures an Access Control List. **Command mode:** Global configuration To view command options, see page 162.
`[no] access-control group` *<1-768>* Configures an ACL Group. **Command mode:** Global configuration To view command options, see page 167.
`show access-control` Displays the current ACL parameters. **Command mode:** All except User EXEC

Access Control List Configuration

These commands allow you to define filtering criteria for each Access Control List (ACL).

Table 4-52 ACL Configuration Commands

Command Syntax and Usage
[no] access-control list {*<1-768>***} egress-port** *<port number>* Configures the ACL to function on egress packets. **Command mode:** Global configuration
access-control list {*<1-768>***} action {permit|deny|set-priority** *<0-7>***}** Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
access-control list {*<1-768>***} statistics** Enables or disables the statistics collection for the Access Control List. **Command mode:** All except User EXEC
default access-control list {*<1-768>***}** Resets the ACL parameters to their default values. **Command mode:** Global configuration
show access-control list *<1-768>* Displays the current ACL parameters. **Command mode:** All except User EXEC

Ethernet Filtering Configuration

These commands allow you to define Ethernet matching criteria for an ACL.

Table 4-53 Ethernet Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list {*<1-768>***} ethernet source-mac-address {***<MAC address>***} {***<MAC mask>***}** Defines the source MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list {*<1-768>***} ethernet destination-mac-address {***<MAC address>***} {***<MAC mask>***}** Defines the destination MAC address for this ACL. **Command mode:** Global configuration

Table 4-53 Ethernet Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list {*<1-768>***} ethernet vlan {***<VLAN ID>***} {***<VLAN mask>***}** Defines a VLAN number and mask for this ACL. **Command mode:** Global configuration
[no] access-control list {*<1-768>***} ethernet ethernet-type {arp|ip|ipv6|mpls|rarp|any|0xXXXX}** Defines the Ethernet type for this ACL. **Command mode:** Global configuration
[no] access-control list {*<1-768>***} ethernet priority** *<0-7>* Defines the Ethernet priority value for the ACL. **Command mode:** Global configuration
default access-control list {*<1-768>***} ethernet** Resets Ethernet parameters for the ACL to their default values. **Command mode:** Global configuration
no access-control list {*<1-768>***} ethernet** Removes Ethernet parameters for the ACL. **Command mode:** Global configuration
show access-control list {*<1-768>***} ethernet** Displays the current Ethernet parameters for the ACL. **Command mode:** All except User EXEC

IP version 4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

Table 4-54 IP version 4 Filtering Configuration Commands

Command Syntax and Usage

`[no] access-control list {`*<1-768>***`} ipv4 source-ip-address`** *<IP address> {<IP mask>*

Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.

Command mode: Global configuration

`[no] access-control list {`*<1-768>***`}ipv4 destination-ip-address`** *<IP address> <IP mask>*

Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.

Command mode: Global configuration

`[no] access-control list {`*<1-768>***`} ipv4 protocol`** *<0-255>*

Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.

Number	Name
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	`vrrp`

Command mode: Global configuration

`[no] access-control list {`*<1-768>***`} ipv4 type-of-service`** *<0-255>*

Defines a Type of Service value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.

Command mode: Global configuration

`default access-control list {`*<1-768>***`} ipv4`**

Resets the IPv4 parameters for the ACL to their default values.

Command mode: Global configuration

`show access-control list {`*<1-768>***`} ipv4`**

Displays the current IPV4 parameters.

Command mode: All except User EXEC

TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 4-55 TCP/UDP Filtering Configuration Commands

Command Syntax and Usage

`[no] access-control list {`*<1-768>***`} tcp-udp source-port`** *<1-65535>* *<mask (0xFFFF)>*

Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:

Number	Name
20	ftp-data
21	ftp
22	ssh
23	telnet
25	smtp
37	time
42	name
43	whois
53	domain
69	tftp
70	gopher
79	finger
80	http

Command mode: Global configuration

`[no] access-control list {`*<1-768>***`} tcp-udp destination-port`** *<1-65535>* *<mask (0xFFFF)>*

Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `sport` above.

Command mode: Global configuration

`[no] access-control list {`*<1-768>***`} tcp-udp flags`** *<flag (0x0-0x3f)>*

Defines a TCP/UDP flag for the ACL.

Command mode: Global configuration

Table 4-55 TCP/UDP Filtering Configuration Commands

Command Syntax and Usage
`default access-control list {<1-768>} tcp-udp` Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
`show access-control list {<1-768>} tcp-udp` Displays the current TCP/UDP Filtering parameters. **Command mode:** All except User EXEC

Packet Format Filtering Configuration

These commands allow you to define Packet Format matching criteria for an ACL.

Table 4-56 Packet Format Filtering Configuration Commands

Command Syntax and Usage
`access-control list {<1-768>} packet-format ethernet {ethertype2|snap|llc}` Defines the Ethernet format for the ACL. **Command mode:** Global configuration
`[no] access-control list {<1-768>} packet-format tagged` Defines the tagging format for the ACL. **Command mode:** Global configuration
`[no] access-control list {<1-768>} packet-format ip {ipv4|ipv6}` Defines the IP format for the ACL. **Command mode:** Global configuration
`default access-control list {<1-768>} packet-format` Resets Packet Format parameters for the ACL to their default values. **Command mode:** Global configuration
`show access-control list {<1-768>} packet-format` Displays the current Packet Format parameters for the ACL. **Command mode:** All except User EXEC

ACL Group Configuration

These commands allow you to compile one or more ACLs into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

Table 4-57 ACL Group Configuration Commands

Command Syntax and Usage
`access-control group {`*<1-768>***`} list`** *<1-768>* Adds the selected ACL to the ACL Group. **Command mode:** Global configuration
`no access-control group {`*<1-768>***`} list`** *<1-768>* Removes the selected ACL from the ACL Group. **Command mode:** Global configuration
`show access-control group` *<1-768>* Displays the current ACL group parameters. **Command mode:** All except User EXEC

ACL Metering Configuration

These commands define the Access Control profile for the selected ACL or ACL Group.

Table 4-58 ACL Metering Configuration Commands

Command Syntax and Usage
`access-control list {`*<1-768>***`} meter action {permit|deny}`** Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets. **Command mode:** Global configuration
`access-control list {`*<1-768>***`} meter committed-rate`** *`<1000-1000000>`* Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
`access-control list {`*<1-768>***`} meter maximum-burst-size`** *`<32-4096>`* Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096 **Command mode:** Global configuration
`[no] access-control list {`*<1-768>***`} meter enable`** Enables or disables ACL Metering. **Command mode:** Global configuration

Table 4-58 ACL Metering Configuration Commands

Command Syntax and Usage
`access-control list {`*<1-768>***`} meter action {drop|pass}`** Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
`show access-control list {`*<1-768>***`} meter`** Displays current ACL Metering parameters. **Command mode:** All

ACL Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL or ACL Group. You can configure different re-mark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

Re-Marking In-Profile Configuration

Table 4-59 Re-Mark Configuration Commands

Command Syntax and Usage
`access-control list {`*<1-768>***`} re-mark in-profile dscp`** *<0-63>* Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value. **Command mode:** Global configuration
`show access-control list {`*<1-768>***`} re-mark`** Displays current Re-Mark In-Profile parameters. **Command mode:** All

Update User Priority Configuration

Table 4-60 User Priority Configuration Commands

Command Syntax and Usage

`access-control list {`*<1-768>***`} re-mark in-profile dot1p`** *<0-7>*

Defines 802.1p value. The value is the priority bits information in the packet structure.

Command mode: Global configuration

`[no] access-control list {`*<1-768>***`} re-mark in-profile use-tos-precedence`**

Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.

Command mode: Global configuration

`show access-control list {`*<1-768>***`} re-mark`**

Displays current Re-Mark In-Profile User Priority parameters.

Command mode: All

Re-Marking Out-of-Profile Configuration

Table 4-61 Out-of-Profile Configuration Commands

Command Syntax and Usage

`access-control list {`*<1-768>***`} re-mark out-profile dscp`** *<0-63>*

Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.

Command mode: Global configuration

`show access-control list {`*<1-768>***`} re-mark`**

Displays current Re-Mark Out-of-Profile parameters.

Command mode: All

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
RS G8000(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via TFTP, as described on page 170.

Saving the Active or Backup Switch Configuration

When the **copy running-config tftp** command is used, the switch's active configuration commands (as displayed using **show running-config**) will be uploaded to the specified script configuration file on the TFTP server. To start the switch configuration upload, at the prompt, enter:

```
RS G8000(config)# copy running-config tftp
```

When the **copy backup-config tftp** command is used, the switch's backup configuration commands (as displayed using **show backup-config**) will be uploaded to the specified script configuration file on the TFTP server. To start the switch configuration upload, at the prompt, enter:

```
RS G8000(config)# copy backup-config {tftp}
```

Restoring the Active or Backup Switch Configuration

When the **`copy active-config running-config`** command is used, the running configuration will be replaced with the commands found in the active (saved) configuration file. The file can contain a full switch configuration or a partial switch configuration.

To restore the active switch configuration, enter:

```
RS G8000# copy active-config running-config
```

When the **`copy tftp running-config`** command is used, the running configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
RS G8000# copy tftp running-config
```

Show Active and Backup Configuration

You can view a summary of the current active and backup configuration.

Table 4-62 Active and Backup Information Commands

Command Syntax and Usage
`show active-config` Displays the parameters set for the active configuration. To view an example of the command output, see page 171. **Command mode:** All
`show backup-config` Displays the parameters set for the backup configuration. **Command mode:** All

Active Configuration command output

The following command displays active configuration information.

show active-config

Command mode: All except User EXEC

```
Active configuration:

May 23 2008 05:03:45 RS G8000:SYSLOG-INFO:INFO  mgmt: console enabled
#
#switch-type "Blade Network Technologies Rack Switch G8000"
#Software Version 6.0.1
#
!
!
spanning-tree stp 1 vlan 2,10,20
interface port 1
pvid 10
!
vlan 10
enable
name "VLAN 10"
member 1
!
interface ip 1
 ipvlan 10
 no dhcp enable
 ip address  127.20.4.230 255.255.0.0
!
ip gateway address 127.20.1.1
ip gateway enable

end
```

CHAPTER 5
Operations Commands

Operations commands generally affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use Operations commands to immediately disable a port, with the understanding that when the switch is reset, the port returns to its normally configured operation.

These commands allow you to alter switch operational characteristics without affecting switch configuration.

Table 5-1 General Operations Command

Command Syntax and Usage
`password` *<1-128 characters>* Allows you to change the password. You must enter the current password in use for validation. **Command Mode**: Privileged EXEC
`clear logging` Clears all Syslog messages. **Command Mode**: Privileged EXEC
`ntp send` Allows you to send requests to the NTP server. **Command Mode**: Privileged EXEC

Operations-Level Port Options

Operations-level port commands are used for temporarily disabling or enabling a port, and for resetting the port.

Table 5-2 Port Operations Commands

Command Syntax and Usage
`interface port` *<port number>* **`shutdown`** Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`no interface port` *<port number>* **`shutdown`** Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`interface port` *<port number>* **`dot1x init`** Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration: ■ **`force unauth`** - the port is placed in unauthorized state, and traffic is blocked. ■ **`auto`** - the port is placed in unauthorized state, then authentication is initiated. ■ **`force auth`** - the port is placed in authorized state, and authentication is not required. **Command Mode**: `Privileged EXEC`
`interface port` {*<port number>*} **`dot1x re-authenticate`** Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as `auto`. **Command Mode**: `Privileged EXEC`
`show interface port` *<port number>* **`operation`** Displays the port interface operational state. **Command Mode**: Privileged EXEC

CHAPTER 6

Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands allow you to perform the following actions:

- Select a switch software image to be used when the switch is next reset.
- Select a configuration block to be used when the switch is next reset.
- Download or uploading a new software image to the switch via TFTP.

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, see "Using SNMP with Switch Images and Configuration Files" on page 183."

The boot options are discussed in the following sections.

The following commands allow you to download/backup software files and configuration files.

Table 6-1 General Boot Commands

Command Syntax and Usage
`copy running-config tftp` Copy the running configuration to a file on the selected TFTP server. **Command Mode**: Privileged EXEC
`copy active-config tftp` Copy the active configuration to a file on the selected TFTP server. **Command Mode**: Privileged EXEC
`copy backup-config tftp` Copy the backup configuration to a file on the selected TFTP server. **Command Mode**: Privileged EXEC
`copy {image1|image2|boot-image} tftp` Copy software image file from the selected flash partition to a TFTP server. **Command Mode**: Privileged EXEC

Table 6-1 General Boot Commands

Command Syntax and Usage
copy tftp active-config Copy configuration file from TFTP server to the active-config partition in the switch. **Command Mode**: Privileged EXEC
copy tftp backup-config Copy configuration file from TFTP server to the backup-config partition in the switch. **Command Mode**: Privileged EXEC
copy tftp image1|image2|boot-image Copy software image file from a TFTP server to the selected flash partition on the switch. **Command Mode**: Privileged EXEC

Stacking Boot commands

The Stacking Boot commands are used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

Table 6-2 Stacking Boot commands

Command Syntax and Usage
boot stack mode [master|member] Configures the Stacking mode for the selected switch. **Command Mode**: Privileged EXEC
boot stack vlan *<VLAN 2-4094>* *<asnum 1-12>*|**master|backup|all** Configures the VLAN used for Stacking control communication. **Command Mode**: Privileged EXEC
default boot stack *<asnum 1-12>*|**master|backup|all** Resets the Stacking boot parameters to their default values. **Command Mode**: Privileged EXEC
boot stack push-image [boot-image|image1|image2] *<asnum 1-12>* Pushes the selected software file from the master to the selected switch. **Command Mode**: Privileged EXEC
show boot stack *<asnum 1-12>*|**master|backup|all** Displays current Stacking boot parameters. **Command Mode**: Privileged EXEC

Updating the Switch Software Image

The switch software image is the executable code running on the switch. A version of the image ships with the switch, and comes pre-installed. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your switch, go to:

http://www.bladenetwork.net/support_services_rackswitch.html

Click on software updates. Use the following command to determine the current software version:

```
RS G8000# show boot
```

To upgrade the software image on your switch, perform the following steps:

- Load the new boot image and software image onto a TFTP server on your network.
- Transfer the new boot image and software image from the TFTP server to your switch.
- Select the new software image to be loaded into switch memory the next time the switch is reset.

Loading new Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot-image`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

Each new software release generally requires a new boot file. Before you attempt to boot the switch with a new software image, load the new boot file, if available.

To load a new software image to your switch, you need the following:

- The boot file and software image loaded on a TFTP server on your network
- The hostname or IP address of the TFTP server
- The name of the new software image or boot file

Note – The DNS parameters must be configured if specifying hostnames.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. **In Privileged EXEC mode, enter the following command:**

```
RS G8000# copy tftp {image1|image2|boot-image}
```

2. **Enter the hostname or IP address of the TFTP server.**

```
Address or name of remote host: <name or IP address>
```

3. **Enter the name of the new software file on the server.**

```
Source file name: <filename>
```

The exact form of the name will vary by server. However, the file location normally is relative to the TFTP directory (usually `tftpboot`).

4. **The system prompts you to confirm your request.**

You should next select a software image to run, as described below.

Selecting a Software Image to run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. **In Global Configuration mode, enter:**

```
RS G8000(config)# boot image {image1|image2}
```

2. **Enter the name of the image you want the switch to use upon the next boot.**

   The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

Uploading a Software Image From Your Switch

You can upload a software image from the switch to a TFTP server.

1. **In Privileged EXEC mode, enter:**

```
RS G8000# copy {<image1|image2>} tftp
```

2. **Enter the name or the IP address of the TFTP server:**

```
Address or name of remote host: <name or IP address>
```

3. **Enter the name of the file into which the image will be uploaded on the TFTP server:**

```
Destination file name: <filename>
```

4. **The system then requests confirmation of what you have entered. To have the file uploaded, enter Y.**

```
image2 currently contains Software Version 1.0.1.0
 that was downloaded at  0:23:39 Thu Apr  1, 2008.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on TFTP server 10.20.10.10
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform a save operation (**`copy running-config active-config`**), your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the factory default. This can be useful when a custom-configured switch is moved to a network environment where it will be re configured for a different purpose.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

In Global Configuration mode, enter:

```
RS G8000 (config)# boot configuration-block {active|backup|factory}
```

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

In Global Configuration mode, enter the following command to reset (reload) the switch:

```
RS G8000 (config)# reload
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.

Confirm reload (y/n) ?
```

Accessing the BLADE OS CLI

To access the Alteon OS CLI, enter the following command from the ISCLI:

```
Router(config)# boot cli-mode aos
```

The default command-line interface for the G8000 is the BLADE OS CLI. To access the ISCLI, enter the following command and reset the switch:

```
Main# boot/mode iscli
```

Users can select the CLI mode upon login, if the following command is enabled:

```
boot cli-mode prompt
```

Only an administrator connected through the CLI can view and enable the `prompt` command. When `prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

Using the Boot Management menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press the **`<Shift>`** key and the **`<B>`** key at the same time. The Boot Management menu appears.

```
Resetting the System ...
Memory Test ...............................

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the boot image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The boot process continues.

Using SNMP with Switch Images and Configuration Files

This section describes how to use MIB calls to work with switch images and configuration files. You can use a standard SNMP tool to perform the actions, using the MIBs listed in Table 6-3.

The examples in this section use the MIB name, but you can also use the OID.

Table 6-3 lists the MIBS used to perform operations associated with the G8000 switch image and configuration files. These MIBS are contained within in the file “g8000.mib”

Table 6-3 MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTftpServer	1.3.6.1.4.1.26543.100.100.17.3.1.0
agTftpImage	1.3.6.1.4.1.26543.100.100.17.3.2.0
agTftpImageFileName	1.3.6.1.4.1.26543.100.100.17.3.3.0
agTftpCfgFileName	1.3.6.1.4.1.26543.100.100.17.3.4.0
agTftpAction	1.3.6.1.4.1.26543.100.100.17.3.5.0
agTftpLastActionStatus	1.3.6.1.4.1.26543.100.100.17.3.6.0

The following SNMP actions can be performed using the MIBs listed in Table 6-3.

- Load a new Switch image (boot or running) from a TFTP server.
- Load a previously saved switch configuration from a TFTP server.
- Save the switch configuration to a TFTP server.

Loading a new switch image

To load a new switch image with the name “MyNewImage.img” into `image2`, follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the switch image resides:**

   ```
   Set agTftpServer.0 “192.168.10.10”
   ```

2. **Set the area where the new image will be loaded:**

   ```
   Set agTftpImage.0 “image2”
   ```

3. **Set the name of the image:**

   ```
   Set agTftpImageFileName.0 “MyNewImage.img”
   ```

4. **Initiate the transfer. To transfer a switch image, enter 2 (get image):**

   ```
   Set agTftpAction.0 “2”
   ```

5. **Verify the transfer:**

   ```
   Get agTftpLastActionStatus.0
   ```

Loading a switch configuration to the active configuration

Use this procedure to load a saved switch configuration (“MyActiveConfig.cfg”) into the active configuration block. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the switch Configuration File resides:**

   ```
   Set agTftpServer.0 “192.168.10.10”
   ```

2. **Set the name of the configuration file:**

   ```
   Set agTftpCfgFileName.0 “MyActiveConfig.cfg”
   ```

3. **Initiate the transfer. To restore a running configuration, enter 12 (get config):**

   ```
   Set agTftpAction.0 “12”
   ```

4. **Verify the transfer:**

   ```
   Get agTftpLastActionStatus.0
   ```

Saving the switch configuration from the active configuration

To save the active switch configuration to a TFTP server follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the configuration file is saved:**

   ```
   Set agTftpServer.0 "192.168.10.10"
   ```

2. **Set the name of the configuration file:**

   ```
   Set agTftpCfgFileName.0 "MyActiveConfig.cfg"
   ```

3. **Initiate the transfer. To save a running configuration file, enter 13 (put config):**

   ```
   Set agTftpAction.0 "13"
   ```

4. **Verify the transfer:**

   ```
   Get agTftpLastActionStatus.0
   ```

CHAPTER 7
Maintenance Commands

Use the maintenance commands to manage dump information and to forward database information. Maintenance commands include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the switch after any one of the following occurs:

- The switch administrator forces a switch *panic*. The **`debug panic`** command causes the switch to dump state information to flash memory, and then causes the switch to reset.
- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reset the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reset.

To use the maintenance commands, you must be logged in to the switch as the administrator.

Table 7-1 General Maintenance Commands

Command Syntax and Usage
`copy flash-dump {ftp|tftp}` Saves the switch dump information to a file on the selected FTP/TFTP server. **Command mode:** All
`clear flash-dump` Deletes all Flash configuration blocks. **Command mode:** All except User EXEC

Table 7-1 General Maintenance Commands

Command Syntax and Usage
`show tech-support` Dumps all switch information, statistics, and configuration. The output default file name is `tsdmp`. **Command mode:** All
`copy tech-support {ftp|tftp}` Saves all switch information, statistics, and configuration to a file on the selected FTP/TFTP server. The output default file name is `tsdmp`. **Command mode:** All

Forwarding Database Maintenance

The Forwarding Database commands can be used to view information, to delete a MAC address from the forwarding database, or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 7-2 FDB Manipulation Commands

Command Syntax and Usage
`show mac-address-table address {`*<MAC address>***`}`** Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the following formats: `xx:xx:xx:xx:xx:xx` format (such as `08:00:20:12:34:56`) or `xxxxxxxxxxxx` format (such as `080020123456`) **Command mode:** All except User EXEC
`show mac-address-table interface port {`*<port number>***`}`** Displays all FDB entries for a particular port. **Command mode:** All except User EXEC
`show mac-address-table vlan {`*<VLAN number>***`}`** Displays all FDB entries on a single VLAN. **Command mode:** All except User EXEC
`show mac-address-table state {forward|trunk|unknown}` Displays all FDB entries of a particular state. **Command mode:** All except User EXEC
`no mac-address-table {`*<MAC address>* | *<VLAN number>***`|all}`** Removes static FDB entries. **Command mode:** All except User EXEC
`show mac-address-table` Displays all entries in the Forwarding Database. **Command mode:** All except User EXEC
`clear mac-address-table` Clears the entire Forwarding Database from switch memory. **Command mode:** All except User EXEC

ARP Cache Maintenance

Table 7-3 Address Resolution Protocol Maintenance Commands

Command Syntax and Usage
`show ip arp find` *<IP address>* Shows a single ARP entry by IP address. **Command mode:** All except User EXEC
`show ip arp interface port` *<port number>* Shows ARP entries on selected ports. **Command mode:** All except User EXEC
`show ip arp vlan` *<1-4095>* Shows ARP entries on a single VLAN. **Command mode:** All except User EXEC
`show ip arp reply` Shows the list of IP addresses which the switch will respond to for ARP requests. **Command mode:** All except User EXEC
`show ip arp` Shows all ARP entries. **Command mode:** All except User EXEC
`clear ip arp-cache` Clears the entire ARP list from switch memory. **Command mode:** All except User EXEC

NOTE – To display all or a portion of ARP entries currently held in the switch, you can also see "ARP Information" on page 55.

IGMP Group Information

Table 7-4 describes the IGMP Snooping maintenance commands.

Table 7-4 IGMP Multicast Group Maintenance Commands

Command Syntax and Usage
`show ip igmp groups address` *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
`show ip igmp vlan` *<1-4094>* Displays groups on a single vlan. **Command mode:** All
`show ip igmp groups interface port` *<port number>* Displays all IGMP multicast groups on a single port. **Command mode:** All
`show ip igmp groups portchannel` *<trunk number>* Displays all IGMP multicast groups on a single trunk group. **Command mode:** All
`show ip igmp groups` Displays information for all multicast groups. **Command mode:** All
`clear ip igmp groups` Clears the IGMP group table. **Command mode:** All except User EXEC

IGMP Multicast Routers Maintenance

Table 7-5 describes the maintenance commands for IGMP multicast routers.

Table 7-5 IGMP Multicast Router Maintenance Commands

Command Syntax and Usage
`show ip igmp mrouter vlan` *<1-4094>* Displays multicast router information for the selected VLAN. **Command mode:** All
`show ip igmp mrouter information` Shows IGMP multicast router information. **Command mode:** All
`clear ip igmp mrouter` Clears all static multicast routers from the switch. **Command mode:** Global configuration

Index

A

abbreviating commands (CLI) 20
access control
  user 126
ACL Port commands 131
ACL statistics 90
active configuration block 101, 180
active switch configuration
  active switch configuration
  restoring 170
  TFTP server 170
administrator account 22

B

backup configuration block 180
boot options menu 175

C

Cisco Ether Channel 143
command (help) 18
commands
  abbreviations 20
  conventions used in this manual 12
  shortcuts 20
  tab completion 20
commands, ISCLI
  modes 15
configuration
  802.1x 138
  DNS, Domain Name System 159
  DSCP 161
  dump command 170
  FDB, Forwarding Database 143
  flow control 130
  NTP, Network Time Protocol 110
  port 128
  port link speed 129
  port mirroring 136
  port trunking 143
  QoS, Quality of Service 160
  save changes 101
  SNMP 110
  VLAN default (PVID) 128
configuration block
  active 180
  backup 180
  factory 180
  selection 180
configuration commands 99
Copy commands 99
COS queue information 61
CPU statistics 93
CPU utilization 93

D

debugging 187
default password 22
disconnect idle timeout 22
downloading software 178
dump
  configuration command 170
  maintenance 187
duplex mode
  link status 23

E

EtherChannel
    as used with port trunking 143

F

factory configuration block 180
FDB statistics 85
flow control 23
    configuring 130
forwarding database (FDB) 187
Forwarding Database Information 44
Forwarding Database Menu 189
forwarding state (FWD) 46

G

Global commands 18

H

help 18
HTTPS 124

I

idle timeout
    overview 22
IEEE standards
    802.1x 50
IGMP Snooping 156
IGMP statistics 88
image
    downloading 178
    software, selecting 179
Information
    IGMP Information 57, 59
    IGMP Multicast Router Information 191
    Trunk Group Information 52
information
    802.1p 61
Information commands 23
IP address
    ARP information 55
IP Information 54, 59
ISCLI commands
    modes 15

L

LACP 146
Layer 2 commands 43
Layer 3 commands 54
link
    speed, configuring 129
Link Aggregation Control Protocol 146
link status 23
    duplex mode 23
    port speed 23, 67
Link Status Information 172
linkt (SNMP option) 112

M

MAC (media access control) address 37, 44, 55, 189
Maintenance Menu 187
Management Processor (MP)
    display MAC address 37
manual style conventions 12
mation 52
media access control. *See* MAC address.
meter
    ACL 167
monitor port 136

N

NTP synchronization 110

O

online help 18
Operations commands 173

P

panic
    switch (and Maintenance Menu option) 187
Password
    user access control 126
password
    administrator account 22
    default 22
    user account 22
passwords 21
ping 18
port configuration 128

port mirroring
  configuration 136
port speed 23, 67
port states
  UNK (unknown) 46
port trunking
  description 143
port trunking configuration 143
portchannel configuration 143
ports
  disabling (temporarily) 130
  information 65
  membership of the VLAN 43, 53
  VLAN ID 23, 65
prisrv
  primary radius server 106
PVID (port VLAN ID) 23, 65

R

RADIUS, configuration
  RADIUS 106
read community string (SNMP option) 111
reference ports 46
re-mark 168
retries
  radius server 106
route statistics 98

S

save (global command) 101
secret
  radius server 106
Secure Shell 105
shortcuts (CLI) 20
SNMP options 111
SNMP statistics 94
SNMPv3 113
software
  image 177
  image file and version 25
Stacking
  boot options 176
  configuration 132
  information 39
Statistics Menu 69
switch
  name and location 37
  resetting 180
system
  contact (SNMP option) 111
  date and time 25
  information 37
  location (SNMP option) 111
System Information 25
system options
  wport 123

T

tab completion (CLI) 20
TACACS+, configuration
  TACACS+ 107
Telnet
  configuring switches using 170
Telnet, system options
  Telnet 123
text conventions 12
TFTP 178
timeout
  radius server 106
timeouts
  idle connection 22
traceroute 19
Trunk Group Information 52
typographic conventions, manual 12

U

unknown (UNK) port state 46
upgrade, switch software 177
user access control configuration 126
user account 22

V

VLAN
  configuration 152
VLAN tagging
  port restrictions 153

VLANs
- information 53
- name 43, 53
- port membership 43, 53
- setting default number (PVID) 128
- tagging 23, 65, 153
- VLAN Number 53

W

watchdog timer 187
wport 123